Nr referencyjny: IN.271.1.2022

Sędziszów, dnia 24.10.2022 r.

Specyfikacja Warunków Zamówienia (SWZ)

I. Nazwa oraz adres Zamawiającego.

Zamawiający:	**Gmina Sędziszów, ul. Dworcowa 20, 28-340 Sędziszów Godziny pracy: poniedziałek 07:30 – 17:00, wtorek- czwartek 07:30- 15:30, piątek 07:30 – 14:00. Tel.: 41 3811 127 adres internetowy: www.bip.sedziszow.pl e-mail: um@sedziszow.pl adres elektronicznej skrzynki podawczej ePUAP: /1kqcvr3465/skrytka**
Prowadzący postępowanie:	**Gmina Sędziszów, ul. Dworcowa 20, 28-340 Sędziszów Godziny pracy: poniedziałek 07:30 – 17:00, wtorek- czwartek 07:30- 15:30, piątek 07:30 – 14:00. Tel.: 41 3811 127 adres internetowy: www.bip.sedziszow.pl e-mail: um@sedziszow.pl adres elektronicznej skrzynki podawczej ePUAP: /1kqcvr3465/skrytka**
Strona prowadzonego postępowania: https://miniportal.uzp.gov.pl/Postepowania Zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postepowaniem o udzielenie zamówienia będą udostępniane na stronie internetowej https://bip.sedziszow.pl/?c=mdPrzetargi-cmPokaz-2437	

II. Tryb udzielenia zamówienia.

1. Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2022r., poz. 1710 ze zm.) [zwanej dalej także „ustawa Pzp”].
2. Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.

Nr referencyjny: IN.271.1.2022

3. Zamawiający w oparciu o zapisy art. 274 ust. 1 ustawy Pzp wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni od dnia wezwania, podmiotowych środków dowodowych jeżeli są wymagane.
4. **Zgodnie z art. 310 ustawy Zamawiający może unieważnić postępowanie o udzielenie zamówienia, jeżeli środki publiczne, które zamawiający zamierzał przeznaczyć na sfinansowanie zamówienia, nie zostały mu przyznane**.

III. Opis przedmiotu zamówienia.

„Zakup sprzętu komputerowego, oprogramowania, szkoleń oraz centralnej platformy e-Usług Mieszkańca w Gminie Sędziszów"

1. Przedmiotem zamówienia jest dostawa sprzętu komputerowego, oprogramowania, szkoleń dla Gminy Sędziszów oraz usług dla Gminy Sędziszów

Część I:

1. Komputery (stacje robocze z monitorami wraz z systemami operacyjnym oraz AIO wraz z systemami operacyjnym)
2. Laptopy
3. Serwery (w jednym przypadku wraz z usługą wdrożenia, a drugi z dodatkowym oprogramowaniem)
4. UPS
5. Skanery dokumentów
6. Monitor
7. Serwery plików
8. Zakup i wdrożenie centralnej platformy e-Usług mieszkańca wraz z dokupieniem modułu do systemu dziedzinowego
9. Zakup oprogramowania
10. Szkolenia pracowników z cyberbezpieczeństwa
11. Zakup zabezpieczeń logicznych (zapory UTM i system analizy UTM)

Zamówienie realizowane jest w ramach konkursu Grantowego **Cyfrowa Gmina** Oś Priorytetowa V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

Część II:
1. Laptopy
2. Pakiet biurowy
3. Oprogramowanie – ochrona stacji roboczych

Zamówienie realizowane jest w ramach umowy o powierzenie grantu nr 2879/2022 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „**Wsparcie dzieci z rodzin pegeerowskich w rozwoju cyfrowym – Granty PPGR**"

Nr referencyjny: IN.271.1.2022

Szczegółowy opis przedmiotu zamówienia, określający minimalne parametry wymagane przez Zamawiającego, znajduje się w **załączniku nr 6 do SWZ**.

2. **Warunki realizacji:**
   Przedmiot zamówienia należy dostarczyć do: **Gmina Sędziszów, ul. Dworcowa 20,28-340 Sędziszów**.
   1) w ilościach i asortymencie zgodnym z opisem przedmiotu zamówienia, wnieść do wskazanego pomieszczenia i dokonać niezbędnych prac w zakresie montażu, rozmieszczenia podłączenia i uruchomienia.
      Przedmiot zamówienia Wykonawca dostarczy własnym środkiem transportu, na własny koszt i ryzyko. Za szkody powstałe w czasie transportu odpowiedzialność ponosi Wykonawca.
   2) Wszelkie dostarczone urządzenia powinny być fabrycznie nowe, nieużywane i obejmować wszystkie wymagania wskazane w SWZ i załącznikach w pełnym podanym zakresie.
   3) Wszystkie dotyczące przedmiotu zamówienia wymagania wskazane w SWZ i załącznikach należy traktować jako minimalne.
   4) Wykonawca zapewni, że dostarczone urządzenia będą spełniać wymagania wynikające z obowiązujących przepisów prawa, w szczególności w zakresie wymaganych atestów, opinii technicznych i dopuszczeni do korzystania na ternie Polski, o ile są wymagane.
   5) Wykonawca winien dysponować odpowiednimi środkami i warunkami technicznymi, potencjałem ekonomicznym i organizacyjnym niezbędnym do realizacji zamówienia.
   6) Zwrot towaru, który nie nadaje się do użytkowania i dostarczenie towaru zamiennego, wolnego od wad i usterek nastąpi na koszt Wykonawcy. Część przedmiotu umowy nie przyjętą w czasie trwania odbioru końcowego Wykonawca wymieni na nową o takich samych parametrach i rodzaju we wskazanym przez Zamawiającego terminie, na własny koszt.

3. 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. Dopuszcza się również wykazanie tej równoważności normami równoważnymi w stosunku do tych wskazanych w OPZ lub powszechnie obowiązujących. Na Wykonawcy spoczywa ciężar wskazania „równoważności". Przy doborze materiałów równoważnych Wykonawca zobowiązany jest zapewnić również osiągnięcie wskaźników określonych w OPZ.

4. **Minimalne warunki gwarancji:**
   1) Wymagany przez Zamawiającego okres gwarancji i rękojmi wynosi:
      dla części I: znajduje się w **załączniku nr 6 do SWZ**, **dla części II:** znajduje się w **załączniku nr 6 do SWZ**.
      Okres rękojmi i gwarancji rozpoczyna się równocześnie dla całości dostawy.
   2) Udzielona gwarancja i rękojmia obejmuje **wszystkie elementy** dostarczonego sprzętu.
   3) W przypadku max 3 napraw gwarancyjnych tego samego wyposażenia, sprzętu/podzespołu Wykonawca będzie zobowiązany dokonać wymiany na nowy wolny od wad.

Nr referencyjny: IN.271.1.2022

4) W ramach udzielonej gwarancji Wykonawca zapewnia autoryzowany serwis techniczny i nie może odmówić wymiany niesprawnej części na nową, w przypadku, gdy jej naprawa nie gwarantuje prawidłowej pracy wyposażenia i sprzętu.
5) Czas reakcji serwisu (fizyczne stawienie się serwisanta w miejscu zainstalowania sprzętu i podjęcie czynności zmierzających do naprawy sprzętu) max w ciągu 72 godzin (pełne godziny) licząc od momentu zgłoszenia awarii.
6) Jeżeli okres naprawy urządzenia będzie dłuższy niż 14 dni należy na ten czas dostarczyć sprawne urządzenie zastępcze z ważnym paszportem technicznym.
7) Wskazane w szczegółowym opisie przedmiotu zamówienia minimalne zapisy muszą być uwzględnione w karcie gwarancyjnej (załącznik do wzoru umowy),
8) Inne wymagania:
   a) Bezpłatna dostawa, wniesienie, instalacja, uruchomienie, testowanie i włączenie do eksploatacji;
   b) Instrukcja obsługi w jęz. polskim w wersji drukowanej;
9) Karta gwarancyjna dostarczana przez wykonawcę nie może nakładać na Zamawiającego dodatkowych zobowiązań finansowych i materialnych, które by uzależniały uprawnienia do udzielonej gwarancji.

5. **Zamawiający przewiduje składanie ofert częściowych. Wykonawca ma prawo złożyć ofertę na dowolną ilość wskazanych części.**

6. Oznaczenie przedmiotu zamówienia wg wspólnego słownika zamówień CPV dla części 1-2

30213000-5 Komputery osobiste
33195100-4 Monitory
30213100-6 Komputery przenośne
48820000-2 Serwery
35100000-5 Urządzenia awaryjne i zabezpieczające
42962000-7 Urządzenia drukujące i graficzne
80550000-4 Usługi szkolenia w dziedzinie bezpieczeństwa
72000000-5 Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia
32420000-3 Urządzenia sieciowe
48000000-8 Pakiety oprogramowania i systemy informatyczne
48310000-4 Pakiety oprogramowania do tworzenia dokumentów

7. W przypadku stwierdzenia rozbieżności w wymaganych warunkach podmiotowych i przedmiotowych oraz wymaganych środkach dowodowych podmiotowych i przedmiotowych w OPZ i SWZ wiążące są postanowienia SWZ.

IV. Termin i miejsce wykonania przedmiotu zamówienia.

1. Wymagany termin realizacji zamówienia:
   Termin dostawy:
   Cześć I: 60 dni kalendarzowych od podpisania umowy.
   Część II: 14 dni kalendarzowych od podpisania umowy.
2. Wymagany termin gwarancji dla:
   części I: min. 24 miesiące,
   części II: min. 24 miesięce

chyba że opis przedmiotu zamówienia wskazuje inaczej. Okres gwarancji i rękojmi rozpoczyna się od daty przekazania zamawiającemu przedmiotu zamówienia potwierdzonego bezusterkowym protokołem odbioru.

3. Okres rękojmi wynosi 24 miesięcy.

V. Podmiotowe i przedmiotowe środki dowodowe.

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy złożą wraz z ofertą oświadczenia a wskazany Wykonawca na żądanie Zamawiającego w terminie nie krótszym niż 5 dni od wezwania, przedłoży wymagane w SWZ dokumenty w zakresie:

   1) spełnienia warunków udziału w postępowaniu
   2) niepodlegania wykluczeniu

2. Oświadczenia o którym mowa w ust. 1 **należy złożyć** zgodnie z odpowiednim wzorem stanowiącym załączniki do SWZ. Oświadczenia te dla podmiotów składających ofertę wspólnie oraz podmiotów udostępniających zasoby składane są oddzielnie dla każdego z tych podmiotów. Oświadczenia wraz z ofertą składane są w formie elektronicznej opatrzone kwalifikowanym podpisem elektronicznym lub postaci elektronicznej opatrzone podpisem zaufanym lub podpisem osobistym.

3. **Uprawnienia do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:**

   W celu potwierdzenia spełniania przez wykonawcę warunków udziału w postępowaniu w zakresie:

   Zamawiający odstępuje od opisu sposobu dokonywania oceny spełnienia warunków w tym zakresie. Zamawiający nie dokona oceny spełnienia warunków udziału w postępowaniu.

4. **Zdolność techniczna lub zawodowa:**

   W celu potwierdzenia spełniania przez wykonawcę warunków udziału w postępowaniu, Zamawiający żąda następujących podmiotowych środków dowodowych w zakresie:

   Zamawiający odstępuje od opisu sposobu dokonywania oceny spełnienia warunków w tym zakresie. Zamawiający nie dokona oceny spełnienia warunków udziału w postępowaniu.

5. **Sytuacja ekonomiczna i finansowa:**

   W celu potwierdzenia spełniania przez wykonawcę warunków udziału w postępowaniu Zamawiający żąda złożenia następujących podmiotowych środków dowodowych:

   Zamawiający odstępuje od opisu sposobu dokonywania oceny spełnienia warunków w tym zakresie. Zamawiający nie dokona oceny spełnienia warunków udziału w postępowaniu.

6. 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:
   a) zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
   b) sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
   c) czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą.
5) Zamawiający ocenia, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu, 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.
6) Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia, wraz z oświadczeniem, o którym mowa w Rozdziale V ust. 1 SWZ, także oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, w zakresie, w jakim wykonawca powołuje się na jego zasoby, zgodnie z katalogiem dokumentów określonych w Rozdziale V SWZ.
7) Wykonawca na wezwanie Zamawiającego składa dokumenty potwierdzające brak podstaw wykluczenia, o których mowa w rozdziale VI SWZ, w odniesieniu do podmiotów na zasobach, których polega oraz dokumenty potwierdzające spełnienie warunków udziału w postępowaniu w zakresie, w jakim Wykonawca powołuje się na jego zasoby.

7. Przedmiotowe środki dowodowe.

1) W celu potwierdzenia spełniania przez Wykonawcę warunków udziału w postępowaniu, Zamawiający żąda złożenia wraz z ofertą następujących przedmiotowych środków dowodowych:

   a) Szczegółowy opis oferowanego przedmiotu zamówienia z podaniem nazwy producenta, modelu, kodu produktu, pozwalający na jednoznaczne potwierdzenie zgodności oferowanego sprzętu z minimalnymi wymaganiami określonymi przez Zamawiającego – załącznik nr 6 do SWZ.
   b) Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami,

technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

c) Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

Zamawiający nie przewiduje możliwość uzupełnienia przedmiotowych środków dowodowych

VI. Podstawy wykluczenia.

1. Na potwierdzenie niepodlegania wykluczeniu Wykonawca składa oświadczenie wraz z ofertą,
   Z postępowania o udzielenie zamówienia wyklucza się Wykonawcę z zastrzeżeniem art. 110 ust. 2 ustawy Pzp.
   1) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
      a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
      b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
      c) o którym mowa w art. 228-230a, art. 250a Kodeksu karnego, w art. 46-48 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 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2021 r. poz. 523, 1292, 1559 i 2054),
      d) 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,
      e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
      f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769),
      g) 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,
      h) 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;
   2) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;

3) 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 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;
4) wobec którego prawomocnie orzeczono zakaz ubiegania sią o zamówienia publiczne;
5) jeżeli Zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi Wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe, chyba że wykażą, że przygotowali te oferty niezależnie od siebie;
6) 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.

2. **Z postępowania o udzielenie zamówienia wyklucza się wykonawców, w stosunku do których zachodzi którakolwiek z okoliczności wskazanych w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, na czas trwania tych okoliczności.**
3. Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia.
4. Zamawiający nie wymaga przedstawienia podmiotowych środków dowodowych na potwierdzenie braku podstaw wykluczenia.

VII. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia

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) Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika jaki zakres rzeczowy zamówienia realizować zamierzają poszczególni wykonawcy.
   3) W celu wykazania niepodlegania wykluczeniu z postępowania o udzielenie zamówienia w rozdziale VI wymagane jest załączenie do oferty oświadczenia i przedłożenia na wezwanie dokumentów dla każdego konsorcjanta oddzielnie.

Nr referencyjny: IN.271.1.2022

VIII. Podwykonawcy.

1. Wykonawca, który zamierza powierzyć wykonanie części usług innej firmie (podwykonawcy) jest zobowiązany do:
   1) określenia w złożonej ofercie (na formularzu oferty – załącznik do SWZ lub na oddzielnym oświadczeniu) informacji jaka część przedmiotu zamówienia będzie realizowana przez podwykonawców z podaniem jego danych jeżeli są znane.
   2) Zamawiający nie wymaga, aby Wykonawca składał dokumenty lub oświadczenia o braku podstaw do wykluczenia odnoszące się do podwykonawcy, który nie udostępnił swoich zasobów.
   3) Za zgodą Zamawiającego Wykonawca może w trakcie realizacji zamówienia zgłosić nowych podwykonawców do realizacji zamówienia.

IX. Informacje o środkach komunikacji elektronicznej, przy użyciu których Zamawiający będzie komunikował się z Wykonawcami, oraz informacje o wymaganiach technicznych i organizacyjnych sporządzania, wysyłania i odbierania korespondencji elektronicznej.

1. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcami odbywa się drogą elektroniczną przy użyciu miniPortalu https://miniportal.uzp.gov.pl, ePUAPu https://epuap.gov.pl/wps/portal
2. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, musi posiadać konto na ePUAP. Wykonawca posiadający konto na ePUAP ma dostęp do *formularzy: złożenia, zmiany, wycofania oferty lub wniosku oraz do formularza do komunikacji.*
3. Wymagania techniczne i organizacyjne wysyłania i odbierania korespondencji elektronicznej przekazywanej przy ich użyciu, opisane zostały w Regulaminie korzystania z miniPortalu dostępnym pod adresem https://miniportal.uzp.gov.pl/WarunkiUslugi oraz Regulaminie ePUAP.
4. Wykonawca przystępując do niniejszego postępowania o udzielenie zamówienia publicznego, akceptuje warunki korzystania z miniPortalu, określone w Regulaminie miniPortalu oraz zobowiązuje się korzystając z miniPortalu przestrzegać postanowień tego regulaminu.
5. Maksymalny rozmiar plików przesyłanych za pośrednictwem dedykowanych formularzy do złożenia i wycofania oferty oraz do komunikacji wynosi 150 MB.
6. Za datę przekazania oferty, oświadczenia, o którym mowa w art. 125 ust. 1 ustawy Pzp, podmiotowych środków dowodowych, przedmiotowych środków dowodowych oraz innych informacji, oświadczeń lub dokumentów, przekazywanych w postępowaniu, przyjmuje się datę ich przekazania na ePUAP.
7. W postępowaniu o udzielenie zamówienia korespondencja (inna niż oferta Wykonawcy i załączniki do oferty) odbywa się elektronicznie za pośrednictwem *dedykowanego formularza dostępnego na ePUAP oraz udostępnionego przez miniPortal (Formularz do komunikacji).* Korespondencja przesłana za pomocą tego formularza nie może być szyfrowana. We wszelkiej korespondencji związanej z niniejszym postępowaniem Zamawiający i Wykonawcy posługują się numerem ogłoszenia (BZP).
8. **Przekazanie korespondencji w sposób opisany w ust. 7 wymaga obowiązkowego poinformowania Zamawiającego o przekazaniu wiadomości na adres e-mail wskazany w rozdziale I „Zamawiający" (niedopełnienie tego obowiązku uznane będzie, jako nieskuteczne przekazanie dokumentów). Zamawiający może również komunikować się z Wykonawcami za pomocą poczty elektronicznej".**
9. Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń

składane są przez Wykonawcę za pośrednictwem *Formularza do komunikacji* jako załączniki. Zamawiający dopuszcza również możliwość składania dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń za pomocą poczty elektronicznej, na adres e-mail wskazany w rozdziale I „Zamawiający". Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgody z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego.

10. Zamawiający nie przewiduje sposobu komunikowania się z Wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej, wskazanych w SWZ.
11. Postępowanie o udzielenie zamówienia prowadzi się w języku polskim.
12. Dokumenty i oświadczenia składane przez wykonawcę powinny być w języku polskim. W przypadku załączenia dokumentów sporządzonych w innym języku niż dopuszczony, wykonawca zobowiązany jest załączyć tłumaczenie na język polski.

X. Osoby uprawnione do porozumiewania się z Wykonawcami.

Osobą uprawnioną do porozumiewania się z Wykonawcami w sprawach formalnoprawnych jest:
- Alojzy Jakóbik, tel. 606-206-214, e-mail: przetargi@kancelariajiz.pl
- Krzysztof Malec, tel. 533-229-999, e-mail: krzysztof@sedziszow.pl

XI. Termin związania ofertą.

1. Wykonawca jest związany ofertą od dnia upływu terminu składania ofert przez okres **30 dni** tj. do **dnia 01.12.2022 r.**
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania oferta 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.

XII. Wymagania dotyczące wniesienia wadium.

Wadium nie jest wymagane

XIII. Zabezpieczenie należytego wykonania umowy.

Zabezpieczenie nie jest wymagane.

XIV. Opis sposobu przygotowania oferty.

1. Oferta musi być sporządzona w języku polskim, w postaci elektronicznej w formacie danych w szczególności: .pdf, .doc, .docx, .rtf, .xps, .odt i opatrzona kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
2. W celu korzystania z systemu miniPortal konieczne jest dysponowanie przez użytkownika urządzeniem teleinformatycznym z dostępem do sieci Internet. Aplikacja działa na Platformie Windows, Mac i Linux.

Nr referencyjny: IN.271.1.2022

3. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą. Poprzez oryginał należy rozumieć dokument podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub osobistym przez osobę/osoby upoważnioną/upoważnione. Poświadczenie za zgodność z oryginałem następuje w formie elektronicznej podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub osobistym przez osobę/osoby upoważnioną/upoważnione.
4. Sposób zaszyfrowania oferty opisany został w Instrukcji użytkownika dostępnej na miniPortalu (odbywa się automatycznie).
5. Do przygotowania oferty konieczne jest posiadanie przez osobę upoważnioną do reprezentowania Wykonawcy kwalifikowanego podpisu elektronicznego, podpisu osobistego lub podpisu zaufanego.
6. Jeżeli na ofertę składa się kilka dokumentów, Wykonawca powinien stworzyć folder, do którego przeniesie wszystkie dokumenty oferty, podpisane kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. Następnie z tego folderu Wykonawca zrobi folder .zip (bez nadawania mu haseł i bez szyfrowania). W kolejnym kroku za pośrednictwem miniPortalu Wykonawca zaszyfruje folder zawierający dokumenty składające się na ofertę.
7. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233), 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.
8. Do oferty należy dołączyć oświadczenie o niepodlegania wykluczeniu w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP).
9. Do przygotowania oferty zaleca się wykorzystanie Formularza Oferty, którego wzór stanowi Załącznik do SWZ. W przypadku, gdy Wykonawca nie korzysta z przygotowanego przez Zamawiającego wzoru, w treści oferty należy zamieścić wszystkie informacje wymagane w Formularzu Ofertowym.
10. **Ofertę należy złożyć z wymaganymi załącznikami:**

Oferta cenowa zgodna z załączonym drukiem „formularza oferty" – załącznik do SWZ, która zawiera cenę wyliczoną w sposób opisany w rozdziale XVII SWZ.
Oświadczenia, o których mowa w rozdziale V ust. 2 SWZ (załącznik do SWZ)
Pełnomocnictwo - Jeżeli oferta wraz z oświadczeniami składana jest przez pełnomocnika należy do oferty załączyć pełnomocnictwo upoważniające pełnomocnika do tej czynności.

Wykonawca, który polega na zasobach innych podmiotów składa wraz z ofertą oświadczenie podmiotu o udostępnieniu zasobów wskazujące na okoliczności opisane w rozdziale V ust. 6 SWZ oraz oświadczenia podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, o których mowa w Rozdziale V ust. 1.
Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika jaki zakres rzeczowy wykonania zamówienia realizować zamierzają poszczególni wykonawcy.
Przedmiotowe środki dowodowe. • **Szczegółowy opis oferowanego przedmiotu zamówienia z podaniem nazwy producenta, modelu, kodu produktu, pozwalający na jednoznaczne potwierdzenie zgodności oferowanego sprzętu z minimalnymi wymaganiami określonymi przez Zamawiającego – załącznik nr 6 do SWZ.**

1) Pełnomocnictwo dla pełnomocnika do reprezentowania w postępowaniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia - dotyczy ofert składanych przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia;
2) Oświadczenie Wykonawcy o niepodlegania wykluczeniu z postępowania - wzór oświadczenia o niepodlegania wykluczeniu stanowi Załącznik nr 4 do SWZ. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenie o niepolegania wykluczeniu składa każdy z Wykonawców;

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

XV. Sposób oraz termin składania ofert.

1. Wykonawca składa ofertę za pośrednictwem Formularza do złożenia lub wycofania oferty dostępnego na ePUAP i udostępnionego również na miniPortalu. Sposób złożenia oferty opisany został w Instrukcji użytkownika dostępnej na miniPortalu.
2. Ofertę wraz z wymaganymi załącznikami należy złożyć w terminie do dnia **02.11.2022** r. do godz. **09:00.**
3. Wykonawca może złożyć tylko jedną ofertę.
4. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.

Nr referencyjny: IN.271.1.2022

5. Wykonawca po przesłaniu oferty za pomocą Formularza do złożenia lub wycofania oferty na „ekranie sukcesu" otrzyma numer oferty generowany przez ePUAP. Ten numer należy zapisać i zachować. Będzie on potrzebny w razie ewentualnego wycofania oferty.
6. Wykonawca przed upływem terminu do składania ofert może wycofać ofertę za pośrednictwem Formularza do wycofania oferty dostępnego na ePUAP i udostępnionego również na miniPortalu. Sposób wycofania oferty został opisany w Instrukcji użytkownika dostępnej na miniPortalu.
7. Wykonawca po upływie terminu do składania ofert nie może wycofać złożonej oferty.,

XVI. Termin otwarcia ofert.

1. Otwarcie ofert nastąpi w dniu **02.11.2022 r.** o godzinie **11:00.**
2. Otwarcie ofert jest niejawne.
3. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
4. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o:
   1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
   2) cenach lub kosztach zawartych w ofertach.
5. W przypadku wystąpienia awarii systemu teleinformatycznego, która spowoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
6. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.

XVII. Sposób obliczenia ceny.

1. Oferta musi zawierać ostateczną, sumaryczną cenę obejmującą wszystkie koszty z uwzględnieniem wszystkich opłat i podatków ewentualnych upustów i rabatów oraz innych kosztów określonych w niniejszej SWZ.
2. Cena musi być podana w złotych polskich cyfrowo i słownie, w zaokrągleniu do drugiego miejsca po przecinku.
3. Rozliczenia między zamawiającym a wykonawcą będą regulowane w złotych polskich.
4. W przypadku rozbieżności pomiędzy ceną podaną cyfrowo a słownie, jako wartość właściwa zostanie przyjęta cena podana cyfrowo
5. 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.**
6. W okolicznościach, o których mowa w ust. 4 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 sposobu oceny ofert.

Nr referencyjny: IN.271.1.2022

1. Przy wyborze oferty Zamawiający będzie się kierował kryteriami określonymi 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 się o wyrażenie takiej zgody do kolejnego Wykonawcy, którego oferta została najwyżej oceniona, chyba, że zachodzą przesłanki do unieważnienia postępowania.
9. Kryteria i ich opis:

Nr kryt.	Opis kryteriów oceny	Znaczenie
	dla części nr I i II	
1	**Cena brutto**	**100 % = 100 pkt.**

l.p.	Kryterium	Znaczenie procentowe kryterium	Maksymalna ilość punktów jakie może otrzymać oferta za dane kryterium
1	**Cena brutto** Liczba punktów = Cn/Cb x 100 gdzie: - Cn – najniższa cena spośród wszystkich ofert nie odrzuconych - Cb – cena oferty badanej - 100 wskaźnik stały	100 %	100 pkt.

XIX. Wykaz podmiotowych środków dowodowych składanych na wezwanie.

Nr referencyjny: IN.271.1.2022

Zamawiający nie wymaga podmiotowych środków dowodowych.

XX. 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:

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

2) Wykonawca zobowiązany jest do złożenia szczegółowej kalkulacji cenowej w rozbici na każdą pozycję określoną w opisie przedmiotu zamówienia

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.

XXI. Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do treści tej umowy.

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

XXII. Zamawiający dopuszcza zmianę zawartej umowy w następujących okolicznościach.

1. Zmiany terminu przewidzianego na zakończenie dostawy w przypadku:
   1) wstrzymania dostawy przez Zamawiającego;
   2) działania siły wyższej (np. klęski żywiołowe, strajki generalne, lub lokalne, epidemie oraz inne uwarunkowania niezależne od producenta materiałów dostarczającego główne materiały lub sprzęt czynniki, które wstrzymały produkcję), mającej bezpośredni wpływ na terminowość wykonania dostawy;
   3) wydłużenie terminu realizacji przedmiotu zamówienia z uwagi na wstrzymanie dostaw uniemożliwiających wykonanie zamówienia w pierwotnym terminie z przyczyn niezawinionych przez Wykonawcę.
2. Zmiana zaoferowanego przedmiotu zamówienia na inny o parametrach tożsamych lub lepszych od przyjętych w ofercie w przypadku wycofania z rynku oferowanego sprzętu. Wymagane jest oświadczenie producenta.
3. Zmiana przepisów prawa, w tym przepisów prawa podatkowego.

Nr referencyjny: IN.271.1.2022

XXIII. Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy.

1. Środki ochrony prawnej przysługują Wykonawcy, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy Pzp.
2. 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.
3. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej opatrzone podpisem zaufanym.
4. Na orzeczenie Krajowej Izby Odwoławczej oraz postanowienie Prezesa Krajowej Izby Odwoławczej, o którym mowa w art. 519 ust. 1 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.
5. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX „Środki ochrony prawnej" ustawy Pzp.

XXIV. 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 udzielenia zamówień powtarzających.

XXV. 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", informuję, że:

- administratorem Pani/Pana danych osobowych jest **Burmistrz Sędziszowa, 28-340 Sędziszów, ul. Dworcowa 20.**
- inspektorem ochrony danych osobowych jest **Pan Cieśla Sylwester,** Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym postępowaniem o udzielenie zamówienia publicznego;
- odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 74 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710 z późn. zm.);
- Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia lub na okres przechowywania tych danych zgodnie z wytycznymi o dofinansowanie ze środków UE;

- obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- posiada Pani/Pan:
  - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
  - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych **;
  - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO ***;
  - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- nie przysługuje Pani/Panu:
  - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
  - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
  - **na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO**.

Jednocześnie Zamawiający przypomina o ciążącym na Pani/Panu obowiązku informacyjnym wynikającym z art. 14 RODO względem osób fizycznych, których dane przekazane zostaną Zamawiającemu w związku z prowadzonym postępowaniem i które Zamawiający pośrednio pozyska od wykonawcy biorącego udział w postępowaniu, chyba że ma zastosowanie co najmniej jedno z włączeń, o których mowa w art. 14 ust. 5 RODO.

* Wyjaśnienie: informacja w tym zakresie jest wymagana, jeżeli w odniesieniu do danego administratora lub podmiotu przetwarzającego istnieje obowiązek wyznaczenia inspektora ochrony danych osobowych.

** Wyjaśnienie: skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.

*** Wyjaśnienie: prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

XVI. Załączniki stanowiące integralną część Specyfikacji (SWZ).

Załącznik nr 1	Formularz oferty
Załącznik nr 2	Wzór umowy
Załącznik nr 3	Oświadczenie wykonawcy o spełnieniu warunków udziału w postępowaniu
Załącznik nr 3a	Oświadczenie podmiotu udostępniającego zasoby o spełnieniu warunków udziału w postępowaniu
Załącznik nr 4	Oświadczenie wykonawcy o wykluczeniu
Załącznik nr 4a	Oświadczenie podmiotu udostępniającego zasoby o wykluczeniu
Załącznik nr 5	Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia
Załącznik nr 6	Szczegółowy opis przedmiotu zamówienia

ZATWIERDZAM

……

Nr referencyjny: IN.271.1.2022

Załącznik nr 1 do SWZ

…… dn. ……2022 r.

……
(Nazwa i adres Wykonawcy)

O F E R T A C E N O W A

Nawiązując do zaproszenia złożenia oferty na realizację zamówienia publicznego na:

„Zakup sprzętu komputerowego, oprogramowania, szkoleń oraz centralnej platformy e-Usług Mieszkańca w Gminie Sędziszów"

zgodnie z wymaganiami określonymi w specyfikacji warunków zamówienia dla tego postępowania składamy niniejszą ofertę:

Za wykonanie przedmiotu zamówienia oferujemy cenę w kwocie łącznej brutto:

Dla części nr I

Termin dostawy i wdrożeń ……

1. Komputery (stacje robocze z monitorami wraz z systemami operacyjnym - 2 szt. oraz AIO wraz z systemami operacyjnym - 2 szt.)

a) Stacje robocze – 2 szt.

Nazwa ……

Gwarancja ……

…… złotych

(słownie:……)

w tym podatek VAT.

b) Monitor – 2 szt.

Nazwa ……

Gwarancja ……

…… złotych

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

(słownie:.....)

w tym podatek VAT.

c) All In One – 2 szt.

Nazwa .....

Gwarancja .....

..... złotych

(słownie:.....)

w tym podatek VAT.

2. Laptopy – 2 szt.

Nazwa .....

Gwarancja .....

..... złotych

(słownie:.....)

w tym podatek VAT.

3. Serwery – łącznie 4 szt.

..... złotych

(słownie:.....)

w tym podatek VAT.

W tym:

a) Serwer I **..... złotych**

+ usługa **..... złotych**

Nazwa .....

Gwarancja .....

b) Serwer II **..... złotych**

Nazwa .....

Gwarancja .....

c) Serwer III **..... złotych**

Nazwa .....

Gwarancja .....

d) oprogramowanie **..... złotych**

Nazwa .....

Wsparcie .....

e) Serwer IV **..... złotych**

4. UPS – 1 szt.

Nazwa .....

Gwarancja .....

..... złotych

(słownie:.....)

w tym podatek VAT.

5. Skanery dokumentów – 3 szt.

Nazwa .....

Gwarancja .....

..... złotych

(słownie:.....)

w tym podatek VAT.

6. Monitor – 1 szt.

Nazwa .....

Gwarancja .....

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

..... złotych

(słownie:.....)

w tym podatek VAT.

7. Serwer plików – łącznie 3 szt.

..... złotych

(słownie:.....)

w tym podatek VAT.

W tym:

a) Serwer plików I – 1 szt. **..... złotych**

Nazwa .....

Gwarancja .....

b) Serwer plików II – 2 szt. **..... złotych**

Nazwa .....

Gwarancja .....

8. Zakup i wdrożenie centralnej platformy e-Usług mieszkańca wraz z dokupieniem modułu do systemu dziedzinowego

a) Centralna Platforma e-Usług Mieszkańca – 1 szt.

Nazwa .....

Wsparcie .....

..... złotych

(słownie:.....)

w tym podatek VAT.

b) Moduł do systemu dziedzinowego Urzędu Miejskiego w Sędziszowie – 1 szt.

Nazwa .....

Wsparcie .....

..... złotych

(słownie:.....)

w tym podatek VAT.

9. Program - Zarządzanie uprawnieniami i licencjami - 1 szt.

Nazwa .....

Wsparcie .....

..... złotych

(słownie:.....)

w tym podatek VAT.

10. Szkolenia pracowników z cyberbezpieczeństwa

Nazwa .....

Okres dostępu do szkoleń .....

..... złotych

(słownie:.....)

w tym podatek VAT.

11. Zakup zabezpieczeń logicznych (zapory UTM)

..... złotych

(słownie:.....)

w tym podatek VAT.

W tym:

a) Zapory UTM - 3 szt. **..... złotych**

Nazwa .....

Gwarancja/czas licencji .....

b) System analizy UTM – 1 szt. **..... złotych**
Nazwa .....

Gwarancja/czas licencji .....

Dla części nr II

Termin dostawy .....

1. Laptopy – 46 szt.

Nazwa .....

Gwarancja .....

..... złotych
(słownie:.....)

w tym podatek VAT.

2. Pakiet biurowy – 46 szt.

Nazwa .....

Czas licencji .....

..... złotych
(słownie:.....)

w tym podatek VAT.

3. Oprogramowanie – ochrona stacji roboczych – 46 szt.

Nazwa .....

Czas licencji .....

..... złotych
(słownie:.....)

w tym podatek VAT.

Nr referencyjny: IN.271.1.2022

UWAGA!
W rozdziale XVII ust. 5 SWZ Zamawiający wymaga złożenia wraz z ofertą informacji o powstaniu zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług (VAT) 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.

Dane dotyczące Wykonawcy:

Imię Nazwisko osoby (osób) upoważnionych do podpisania umowy:

……

Numer telefonu: …./ ……

Numer faksu: …./ ……

Numer REGON: …… Numer NIP: ……

Adres kontaktowy e-mail: ……

UWAGA; proszę podać czytelny; adres e-mail i nr faksu na który wykonawca będzie otrzymywał od zamawiającego wszystkie informacje związane z prowadzonym postępowaniem po otwarciu ofert. W związku z przysługującymi środkami ochrony prawnej wykonawcy, liczonymi od dnia przekazania informacji należy upewnić się, że podany adres e-mailowy i podany nr faksu funkcjonuje w sposób poprawny.

3. Warunki płatności będą zgodne z wzorem umowy będącym załącznikiem do SWZ.
4. Oświadczamy, że zapoznaliśmy się ze specyfikacją warunków zamówienia, w tym z wzorem umowy w sprawie zamówienia publicznego i uzyskaliśmy wszelkie informacje niezbędne do przygotowania niniejszej oferty. Przedstawione w specyfikacji warunków zamówienia warunki zawarcia umowy oraz wzór umowy zostały przez nas zaakceptowane.
5. Oświadczamy, że uważamy się za związanych niniejszą ofertą przez czas wskazany w specyfikacji warunków zamówienia.
6. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.**
7. W przypadku uznania niniejszej oferty za ofertę najkorzystniejszą zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego, a przed zawarciem umowy wniesienia zabezpieczenia należytego wykonania umowy.
8. Informuję, że **jestem** (niepotrzebne skreślić) **mikro/małym/średnim/dużym* przedsiębiorcą.**
9. Oferta wraz z załącznikami została złożona na **…….** stronach kolejno ponumerowanych od nr **……** do nr **……**
10. Załącznikami do niniejszej oferty są:

    ……

    ……

* niepotrzebne skreślić

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

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

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

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

Nr referencyjny: IN.271.1.2022

Załącznik nr 2 do SWZ

U m o w a nr .....

zawarta w dniu ……. 2022 roku w Sędziszowie
pomiędzy:

Gmina Sędziszów,
ul. Dworcowa 20,
28-340 Sędziszów
REGON: ……..
zwanym dalej w tekście umowy Zamawiającym

a
Firmą ……..(nazwa i adres Wykonawcy), wpisaną do Krajowego Rejestru Sądowego pod nr: ……. Przez…….. (lub Centralnej Ewidencji i Informacji o Działalności Gospodarczej) NIP: ……., REGON:……..,
reprezentowaną przez
……..,
zwaną w treści umowy „Wykonawcą".

§ 1

1. Zamawiający kupuje, a Wykonawca sprzedaje sprzęt komputerowy w ramach postępowania pn. **„Zakup sprzętu komputerowego, oprogramowania, szkoleń oraz centralnej platformy e-Usług Mieszkańca w Gminie Sędziszów"**
2. Przedmiotu zamówienia realizowany jest w ramach:

Część I*:

Punkt: Podpunkt:

konkursu Grantowego Cyfrowa Gmina Oś Priorytetowa V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia.

Część II- *:

Punkt:

umowy o powierzenie grantu nr 2879/2022 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Wsparcie dzieci z rodzin pegeerowskich w rozwoju cyfrowym – Granty PPGR"

Sprzęt komputerowy zwany w dalszej części umowy sprzętem dostarczone będą w ilościach i rodzajach oraz zgodnie z wymogami określonymi w szczegółowym opisie przedmiotu zamówienia, stanowiący **załącznik nr 6** do Specyfikacji Warunków Zamówienia, zwanej dalej charakterystyką**.**

§2

* Zamawiający pozostawi zapisy dla danego zadania

1. Wykonawca dostarczy, wdroży i dokona niezbędnych prac w terminie **do ..... dni kalendarzowych od momentu podpisania umowy.**
2. Wykonawca zapewni takie opakowanie sprzętu, jakie jest wymagane by nie dopuścić do uszkodzenia lub pogorszenia jego jakości, w trakcie transportu do miejsca dostawy.
3. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
4. Wykonawca umożliwi Zamawiającemu sprawdzenie sprzętu w celu jego odbioru w miejscu dostawy.
   Sprawdzenie sprzętu będzie polegało na upewnieniu się, że sprzęt jest wolny od wad fizycznych, a w szczególności, że sprzęt odpowiada wymogom określonym w charakterystyce.
   Na okoliczność odbioru przedmiotu dostawy zostanie sporządzony protokół odbioru podpisany przez uprawnionych przedstawicieli Zamawiającego i Wykonawcy.
5. Wykonawca wyda Zamawiającemu dokumenty, które dotyczą sprzętu, przede wszystkim karty gwarancyjne na sprzęt i instrukcje obsługi sprzętu oraz oprogramowanie.
   Korzyści i ciężary związane ze sprzętem oraz niebezpieczeństwo przypadkowej utraty lub uszkodzenia sprzętu przechodzą na Zamawiającego z chwilą wydania sprzętu Zamawiającemu. Za dzień wydania sprzętu zamawiającemu uważa się dzień, w którym sprzęt został odebrany przez Zamawiającego, potwierdzony protokołem odbioru.

§ 3

1. Strony ustalają cenę za przedmiot umowy **za część nr** …..... na podstawie oferty w kwocie:
   - **…… zł brutto** (słownie: ……), w tym podatek VAT……zł
   Cena obejmuje koszty transportu, wniesienia i montażu.
2. Zapłata ceny nastąpi po otrzymaniu przez Zamawiającego faktury VAT wraz z protokołem odbioru, przelewem na konto bankowe Wykonawcy wskazane w fakturze.
3. Płatność będzie dokonana po potwierdzeniu przez Zamawiającego pisemnym protokołem odbioru prawidłowo dostarczonego sprzętu.
4. Zamawiający dokona zapłaty w terminie **30 dni** od daty otrzymania prawidłowo wystawionej faktury.
5. Za datę zapłaty strony przyjmują datę obciążenia rachunku Zamawiającego.
6. **Wykonawca w dniu podpisania umowy przedłoży kalkulacje cen jednostkowych zaoferowanych urządzeń.**
7. Wprowadza się następujące zasady dotyczące płatności wynagrodzenia należnego dla Wykonawcy z tytułu realizacji Umowy z zastosowaniem mechanizmu podzielonej płatności:
   1) Zamawiający zastrzega sobie prawo rozliczenia płatności wynikających z umowy za pośrednictwem metody podzielonej płatności (ang. split payment) przewidzianego w przepisach ustawy o podatku od towarów i usług.
   2) Wykonawca oświadcza, że rachunek bankowy na który będą dokonywane płatności to nr……..
      a) jest rachunkiem umożliwiającym płatność w ramach mechanizmu podzielonej płatności, o którym mowa powyżej.
      b) jest rachunkiem znajdującym się w elektronicznym wykazie podmiotów prowadzonym od 1 września 2019 r. przez Szefa Krajowej Administracji Skarbowej, o którym mowa w ustawie o podatku od towarów i usług.

3) W przypadku gdy rachunek bankowy wykonawcy nie spełnia warunków określonych w pkt. 2, opóźnienie w dokonaniu płatności w terminie określonym w umowie, powstałe wskutek braku możliwości realizacji przez Zamawiającego płatności wynagrodzenia z zachowaniem

mechanizmu podzielonej płatności bądź dokonania płatności na rachunek objęty wykazem, nie stanowi dla Wykonawcy podstawy do żądania od Zamawiającego jakichkolwiek odsetek/odszkodowań lub innych roszczeń z tytułu dokonania nieterminowej płatności.

4) Strony postanawiają, że nie jest dopuszczalny bez zgody Zamawiającego przelew wierzytelności z tytułu wynagrodzenia za zrealizowany przedmiot umowy na osobę trzecią.

§ 4

1. Wykonawca udziela niniejszym gwarancji na okres **…….. miesięcy** na przedmiot dostawy na warunkach określonych w SWZ
2. Wykonawca udziela także rękojmi na okres: …… miesięcy.
3. Gwarancja obejmuje wszystkie elementy dostarczonego sprzętu wraz z niezbędnym wyposażeniem z wyłączeniem materiałów eksploatacyjnych podlegających zużyciu podczas normalnej eksploatacji.
4. W okresie gwarancji Wykonawca zapewnia serwis techniczny i nie może odmówić wymiany niesprawnej części na nową w przypadku, gdy jej naprawa nie gwarantuje prawidłowej pracy sprzętu.
5. W przypadku max. 3 napraw gwarancyjnych tego samego wyposażenia, sprzętu/podzespołu Wykonawca będzie zobowiązany dokonać jego wymiany na nowy, wolny od wad.
6. **Wykonawca zapewnia pełny, bezpłatny przegląd okresowy całego sprzętu na 1 miesiąc przed upływem terminu gwarancji.**
7. Zamawiający z tytułu rękojmi może żądać usunięcia wady, jeżeli ujawniła się ona w czasie trwania rękojmi. Zamawiający może wykonywać uprawnienia z tytułu rękojmi po upływie okresu trwania rękojmi, jeżeli zawiadomił Wykonawcę o wadzie przed jego upływem.
8. Zamawiający może według swojego wyboru, wykonywać uprawnienia z tytułu rękojmi albo gwarancji.
9. Na podstawie uprawnień wynikających z tytułu rękojmi lub gwarancji Zamawiający może żądać usunięcia wady, wyznaczając Wykonawcy w tym celu odpowiedni, technicznie uzasadniony termin z zagrożeniem, że po bezskutecznym upływie terminu może usunąć wady na koszt i ryzyko Wykonawcy wybierając w tym celu dowolny podmiot. Koszty poniesione przez Zamawiającego z tego tytuły powiększone o kary umowne wynikające z przedmiotowej umowy, mogą być potrącane przez Zamawiającego z wierzytelności Wykonawcy lub Wykonawca zostanie obciążony na podstawie faktury VAT wystawionej przez Zamawiającego.
10. Czas reakcji serwisu (fizyczne stawienie się serwisanta w miejscu montażu wyposażenia i podjęcie czynności zmierzających do naprawy) powinno nastąpić max. w ciągu **72 godzin** (pełne godziny) licząc od momentu zgłoszenia awarii (usterki).
11. Naprawa zgłoszonej awarii lub usterki (usunięcie wady) powinno nastąpić maksymalnie w ciągu 14 dni roboczych od dnia jej zgłoszenia
12. W przypadku konieczności transportu uszkodzonego sprzętu, transport na koszt własny zapewnia Wykonawca.
13. Zgłoszenie awarii lub wady następuje telefonicznie/faxem na numer telefonu/faxu ……., luba na adres e-mail: ……..
14. W czasie obowiązywania udzielonej gwarancji lub rękojmi Wykonawca na własny koszt dojeżdża do miejsca w którym znajduje się uszkodzony sprzęt.

15. W przypadku istotnej naprawy sprzętu, termin gwarancji oraz rękojmi całego sprzętu, o których mowa w ust. 1 i ust. 2, zaczyna swój bieg na nowo od daty zakończenia skutecznej naprawy. W przypadku naprawy wiążącej się z wymianą części, termin gwarancji i rękojmi na wymienione części równy jest okresom, o których mowa w ust. 1 i ust. 2, i rozpoczyna swój bieg od daty wymiany części.
16. Wykonawca oświadcza, że rozbudowa zakupionego sprzętu o dodatkowe elementy, w celu zachowania uprawnień wynikających z rękojmi lub gwarancji, wymaga zgody Wykonawcy. Bez uzasadnionych powodów Wykonawca nie może odmówić takiej zgody. W przypadku brak odpowiedzi przez Wykonawcę w terminie 14 dni, uważa się że Wykonawca wyraził zgodę na rozbudowę.
17. Wykonawca na zlecenie Zamawiającego zapewni odpłatny serwis pogwarancyjny przez okres 3 lat po ustaniu gwarancji.
18. W przypadku, gdy Wykonawca nie usunie wady w terminie wskazanym w ust. 10 Zamawiający może zlecić jej usunięcie innemu podmiotowi na koszty i ryzyko Wykonawcy.

§ 5

1. W przypadku niewykonania lub nienależytego wykonania umowy przez Wykonawcę Zamawiający może naliczyć karę umowną w następujących przypadkach i wysokościach:
   a. za zwłokę w przekazaniu przedmiotu umowy w wysokości 5 % ceny dla danej części, o której mowa w § 3 ust. 1 umowy za każdy dzień zwłoki,
   b. za zwłokę w usunięciu wad stwierdzonych przy odbiorze lub w okresie gwarancji w wysokości 1 % ceny dla danej części, o której mowa w § 3 ust. 1 umowy za każdy dzień zwłoki licząc od dnia wyznaczonego na usunięcie wad.
   c. za odstąpienie od umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy w wysokości 10 % ceny dla danego zadania o którym mowa w § 3 ust. 1
2. O nałożeniu kary umownej, jej wysokości i podstawie jej nałożenia Zamawiający będzie informował Wykonawcę pisemnie w terminie 14 dni od zaistnienia zdarzenia stanowiącego podstawę nałożenia kary.
3. Maksymalny wymiar kar, o których mowa wyżej nie może przekroczyć 25 % kwoty łącznego wynagrodzenia brutto określonego w § 3 ust. 1 umowy.
4. Zamawiający zastrzega sobie prawo dochodzenia odszkodowania uzupełniającego na zasadach ogólnych Kodeksu Cywilnego, jeżeli wartość powstałej szkody przekroczy wysokość kary umownej.

§ 6

Zamawiającemu przysługuje prawo odstąpienia od umowy w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy (zgodnie z art. 455 Ustawy Prawo Zamówień Publicznych).

§ 7

Zmiana postanowień niniejszej umowy może nastąpić za zgodą obu stron z poszanowaniem zapisów art. 455 ust. 1 Ustawy Prawo Zamówień Publicznych wyrażoną na piśmie pod rygorem nieważności takiej zmiany.

§ 8

Właściwym do rozpoznania sporów wynikłych na tle realizacji niniejszej umowy jest sąd powszechny właściwy dla siedziby Zamawiającego.

Nr referencyjny: IN.271.1.2022

§ 9

1. W sprawach nieuregulowanych niniejszą umową obowiązują przepisy Kodeksu Cywilnego i Ustawy z dnia 11 września 2019 r. Prawo Zamówień Publicznych.
2. Integralne części niniejszej umowy stanowią:
   a) Protokół odbioru – wzór,
   b) Karta gwarancyjna – wzór.

§ 10

Umowa niniejsza sporządzona została w **2 jednobrzmiących** egzemplarzach, po 1 egzemplarzu dla każdej ze stron.

ZAMAWIAJĄCY **WYKONAWCA**

Nr referencyjny: IN.271.1.2022

Sadowie, dnia ……

WZÓR

PROTOKÓŁ ODBIORU z dnia ……

Dostawca: ……..

……..

……..

Odbiorca: ……..

Miejsce odbioru: **……**

Data odbioru: ……..

Dostarczono:

Nazwa	Producent	Nr wersji	Ilość	Cena jednostkowa	Wartość

Strony oświadczają, że przedmiot zamówienia został/ nie został* przez Wykonawcę zrealizowany zgodnie z postanowieniami SWZ, ofertą Wykonawcy oraz funkcjonuje prawidłowo, a dostawa została zrealizowana zgodnie/niezgodnie* z zapisami umowy nr ……., z dnia ……

Strona odbierająca potwierdza, że wyżej wymienione przedmioty/urządzenia zostały odebrane bez zastrzeżeń, jako w pełni sprawne przez uprawnionych pracowników.*

Strona odbierająca stwierdza, że nie dokonała odbioru z przyczyn określonych w uwagach do protokołu.*
Protokół spisano w dwóch jednobrzmiących egzemplarzach.

Strona przekazująca:
……
(podpis i pieczęć)

Strona odbierająca:
……..
(podpis i pieczęć)

UWAGI

……
……
……
……

Strona przekazująca:
……
(podpis i pieczęć)

Strona odbierająca:
……..
(podpis i pieczęć)

* *niepotrzebne skreślić*

Nr referencyjny: IN.271.1.2022

ZAŁACZNIK do Umowy……

KARTA GWARANCYJNA

Data wydania: ……..
Dostawca: ……..
Odbiorca: ……..
Nazwa sprzętu ……..
Numer seryjny: ……..

1. Odpowiedzialność z tytułu gwarancji obejmuje wady powstałe z przyczyn tkwiących w sprzedanym sprzęcie. W ramach gwarancji Wykonawca zobowiązany jest do bezpłatnego usunięcia wad fizycznych.
2. Wykonawca udziela gwarancji z bezpłatnym serwisem na okres **...** miesięcy, licząc od daty podpisania bezusterkowego protokołu odbioru.
3. Wykonawca udziela rękojmi na okres **..... miesięcy**, licząc od daty podpisania bezusterkowego protokołu odbioru.
4. Zamawiający z tytułu rękojmi może żądać usunięcia wady, jeżeli ujawniła się ona w czasie trwania rękojmi. Zamawiający może wykonywać uprawnienia z tytułu rękojmi po upływie okresu trwania rękojmi, jeżeli zawiadomił Wykonawcę o wadzie przed jego upływem.
5. Zamawiający może według swojego wyboru, wykonywać uprawnienia z tytułu rękojmi albo gwarancji.
6. Na podstawie uprawnień wynikających z tytułu rękojmi lub gwarancji Zamawiający może żądać usunięcia wady, wyznaczając Wykonawcy w tym celu odpowiedni, technicznie uzasadniony termin z zagrożeniem, że po bezskutecznym upływie terminu może usunąć wady na koszt i ryzyko Wykonawcy wybierając w tym celu dowolny podmiot. Koszty poniesione przez Zamawiającego z tego tytuły powiększone o kary umowne wynikające z przedmiotowej umowy, mogą być potrącane przez Zamawiającego z wierzytelności Wykonawcy lub Wykonawca zostanie obciążony na podstawie faktury VAT wystawionej przez Zamawiającego.
7. Gwarancja obejmuje wszystkie elementy dostarczonego sprzętu wraz z wyposażeniem, z wyłączeniem materiałów eksploatacyjnych podlegających zużyciu podczas normalnej eksploatacji.
8. W ramach udzielonej gwarancji Wykonawca zapewnia serwis techniczny i nie może odmówić wymiany niesprawnej części na nowa, w przypadku, gdy jej naprawa nie gwarantuje prawidłowej pracy sprzętu.
9. W przypadku maksymalnie 3 napraw gwarancyjnych tego samego urządzenia/podzespołu, Wykonawca będzie zobowiązany do wymiany naprawianego urządzenia/podzespołu na nowy, wolny od wad.
10. Koszty dojazdu serwisu do i z miejsca użytkowania sprzętu lub przewóz uszkodzonego przedmiotu zamówienia do i po naprawie nie obciążają Zamawiającego w okresie gwarancyjnym. Transport uszkodzonego sprzętu, zapewnia Wykonawca.
11. Na 1 miesiąc przed upływem terminu gwarancji, Wykonawca zapewnia pełny, bezpłatny przegląd okresowy całego dostarczonego wyposażenia.
14. W przypadku naprawy sprzętu, termin gwarancji oraz rękojmi o których mowa w ust. 2 i ust. 3 ulega przedłużeniu o czas pozostawania sprzętu w naprawie. W przypadku naprawy wiążącej się z wymianą części, termin gwarancji i rękojmi na wymienione części równy jest okresom, o których mowa w ust. 2 i ust. 3 i rozpoczyna swój bieg od daty wymiany części.
15.Czas reakcji serwisu (fizyczne stawienie się serwisanta w miejscu dostawy wyposażenia i podjęcie czynności zmierzających do naprawy wyposażenia) max w ciągu 72 godzin (pełne godziny) licząc od momentu zgłoszenia awarii (usterki).

16. W przypadku konieczności transportu uszkodzonego sprzętu, transport na koszt własny zapewnia Wykonawca.
17. Zgłoszenie awarii lub wady następuje telefonicznie/faxem na numer telefonu/faxu …….. lub na adres e-mail: ……..
18. W czasie obowiązywania udzielonej gwarancji lub rękojmi Wykonawca na własny koszt dojeżdża do uszkodzonego sprzętu.
19. W przypadku istotnej naprawy sprzętu, termin gwarancji oraz rękojmi całego sprzętu, o których mowa w ust. 1 i ust. 2, zaczyna swój bieg na nowo od daty zakończenia skutecznej naprawy.
W przypadku naprawy wiążącej się z wymianą części, termin gwarancji i rękojmi na wymienione części równy jest okresom, o których mowa w ust. 1 i ust. 2, i rozpoczyna swój bieg od daty wymiany części.
20. Wykonawca oświadcza, że rozbudowa zakupionego sprzętu o dodatkowe elementy, w celu zachowania uprawnień wynikających z rękojmi lub gwarancji, wymaga zgody Wykonawcy. Bez uzasadnionych powodów Wykonawca nie może odmówić takiej zgody. Udzielenie odpowiedzi przez Wykonawcę w sprawie wyrażenia zgody lub jej odmowy powinno nastąpić w ciągu 14 dni od daty wystąpienia przez Zamawiającego.

Nr referencyjny: IN.271.2022

Załącznik nr 3 do SWZ

Zamawiający:

Gmina Sędziszów,
ul. Dworcowa 20,
28-340 Sędziszów

Wykonawca:

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

reprezentowany przez:

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

Oświadczenie Wykonawcy

składane na podstawie art. 125 ust. 1 ustawy z dnia 11.09.2019 r.
Prawo zamówień publicznych (dalej jako: ustawa Pzp),

DOTYCZĄCE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Zakup sprzętu komputerowego, oprogramowania, szkoleń oraz centralnej platformy e-Usług Mieszkańca w Gminie Sędziszów”** prowadzonego przez **Gmina Sędziszów, ul. Dworcowa 20, 28-340 Sędziszów**, oświadczam, co następuje:

INFORMACJA DOTYCZĄCA WYKONAWCY:

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez Zamawiającego w rozdziale V SWZ.

…….. *(miejscowość),* dnia …….. r.

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

Nr referencyjny: IN.271.2022

INFORMACJA W ZWIĄZKU Z POLEGANIEM NA ZASOBACH INNYCH PODMIOTÓW:

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez Zamawiającego w rozdziale V SWZ polegam na zasobach następującego/ych podmiotu/ów: ……

……,

w następującym zakresie: ……

…… *(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu).*

…….. *(miejscowość),* dnia …….. r.

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

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

…….. *(miejscowość),* dnia …….. r.

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

Nr referencyjny: IN.271.1.2022

Załącznik nr 3a do SWZ

Zamawiający:

Gmina Sędziszów,
ul. Dworcowa 20,
28-340 Sędziszów

Wykonawca:

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

reprezentowany przez:

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

Oświadczenie Podmiotu udostępniającego zasoby

(jeżeli dotyczy)

składane na podstawie art. 125 ust. 1 ustawy z dnia 11.09.2019 r.

Prawo zamówień publicznych (dalej jako: ustawa Pzp),

DOTYCZĄCE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Zakup sprzętu komputerowego, oprogramowania, szkoleń oraz centralnej platformy e-Usług Mieszkańca w Gminie Sędziszów”** prowadzonego przez **Gmina Sędziszów, ul. Dworcowa 20, 28-340 Sędziszów**, oświadczam, co następuje:

INFORMACJA DOTYCZĄCA PODMIOTU UDOSTĘPNIAJĄCEGO ZASOBY:

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez Zamawiającego w rozdziale V SWZ.

…….. *(miejscowość),* dnia …….. r.

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

Nr referencyjny: IN.271.1.2022

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

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

…….. *(miejscowość),* dnia …….. r.

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

Nr referencyjny: IN.271.1.2022

Załącznik nr 4 do SWZ

Zamawiający:

Gmina Sędziszów,
ul. Dworcowa 20,
28-340 Sędziszów

Wykonawca:

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

reprezentowany przez:

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

Oświadczenie Wykonawcy

składane na podstawie art. 125 ust. 1 ustawy z dnia 11.09.2019 r.
Prawo zamówień publicznych (dalej jako: ustawa Pzp),

DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Zakup sprzętu komputerowego, oprogramowania, szkoleń oraz centralnej platformy e-Usług Mieszkańca w Gminie Sędziszów”** prowadzonego przez **Gmina Sędziszów, ul. Dworcowa 20, 28-340 Sędziszów**, oświadczam, co następuje:

INFORMACJA DOTYCZĄCA WYKONAWCY:

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.
3. Oświadczam, że nie podlegam wykluczeniu z postępowania w związku z okolicznościami wskazanymi w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, na czas trwania tych okoliczności.

…….. *(miejscowość),* dnia …….. r.

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

Nr referencyjny: IN.271.1.2022

Oświadczam, **że zachodzą** 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 podjąłem następujące środki naprawcze:

……

…….. *(miejscowość),* dnia …….. r.

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

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

…….. *(miejscowość),* dnia …….. r.

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

Nr referencyjny: IN.271.1.2022

Załącznik nr 4a do SWZ

Zamawiający:

Gmina Sędziszów,
ul. Dworcowa 20,
28-340 Sędziszów

Wykonawca:

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

reprezentowany przez:

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

Oświadczenie Podmiotu udostępniającego zasoby (jeżeli dotyczy)

składane na podstawie art. 125 ust. 1 ustawy z dnia 11.09.2019 r. Prawo zamówień publicznych (dalej jako: ustawa Pzp),

DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Zakup sprzętu komputerowego, oprogramowania, szkoleń oraz centralnej platformy e-Usług Mieszkańca w Gminie Sędziszów"** prowadzonego przez **Gmina Sędziszów, ul. Dworcowa 20, 28-340 Sędziszów** , oświadczam, co następuje:

INFORMACJA DOTYCZĄCA PODMIOTU UDOSTĘPNIAJĄCEGO ZASOBY:

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.
3. Oświadczam, że nie podlegam wykluczeniu z postępowania w związku z okolicznościami wskazanymi w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, na czas trwania tych okoliczności.

…….. *(miejscowość),* dnia …….. r.

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

Nr referencyjny: IN.271.1.2022

Oświadczam, **że zachodzą** 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 podjąłem następujące środki naprawcze:

……

…….. *(miejscowość),* dnia …….. r.

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

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

…….. *(miejscowość),* dnia …….. r.

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

Nr referencyjny: IN.271.1.2022

Załącznik nr 5 do SWZ

Zamawiający:

Gmina Sędziszów,
ul. Dworcowa 20,
28-340 Sędziszów

Wykonawca:

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

reprezentowany przez:

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

Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia

składane na podstawie art. 117 ust. 4 ustawy z dnia 11.09.2019 r.
Prawo zamówień publicznych (dalej jako: ustawa Pzp),

DOTYCZĄCE REALIZACJI ZAKRESU PRZEDMIOTU ZAMÓWIENIA PRZEZ POSZCZEGÓLYCH WYKONAWCÓW

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Zakup sprzętu komputerowego, oprogramowania, szkoleń oraz centralnej platformy e-Usług Mieszkańca w Gminie Sędziszów”** prowadzonego przez **Gmina Sędziszów, ul. Dworcowa 20, 28-340 Sędziszów**, oświadczam, co następuje:

•Wykonawca……
(nazwa i adres Wykonawcy)
zrealizuje następujący **kluczowy zakres** przedmiotu zamówienia**: ……**……

……

•Wykonawca……
(nazwa i adres Wykonawcy)
zrealizuje następujący zakres przedmiotu zamówienia:……

……

•Wykonawca……
(nazwa i adres Wykonawcy)
zrealizuje następujący zakres przedmiotu zamówienia:……

……

……..*(miejscowość),*dnia……..r.

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

Nr referencyjny: IN.271.1.2022

Załącznik nr 6 do SWZ

Sędziszów dn. 24.10.2022 r.

Szczegółowy opis przedmiotu zamówienia

„Zakup sprzętu komputerowego, oprogramowania, szkoleń oraz centralnej platformy e-Usług Mieszkańca w Gminie Sędziszów”

Dla części nr I

1. Komputery (stacje robocze z monitorami wraz z systemami operacyjnym - 2 szt. oraz AIO wraz z systemami operacyjnym - 2 szt.)

a) Stacje robocze – 2 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 19505 punktów, załączyć do oferty wyniki przeprowadzonego testu.
Pamięć RAM	8GB DDR4 non-ECC możliwość rozbudowy do min 64GB, min. 1 slot wolny
Pamięć masowa	M.2 256GB NVMe PCIex4
Napęd optyczny	Nagrywarka DVD +/-RW o prędkości min. 8x
Wydajność grafiki	Zintegrowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 1630 punktów w G3D Rating, wynik dostępny na stronie: http://www.videocardbenchmark.net/gpu_list.php
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, port audio combo (słuchawki i mikrofon) na panelu przednim, na tylnym port audio out Wbudowany czytnik kart SD nie zajmujący wnęk zewnętrznych ani wewnętrznych ani slotów na płycie głównej.
Obudowa	Typu SFF z obsługą kart rozszerzeń o niskim profilu, napęd optyczny w dedykowanej wnęce zewnętrznej slim. Suma wymiarów mierzona po krawędziach obudowy nie może przekraczać 680 mm, waga max 6kg, Zasilacz o mocy max. 180W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%. Wbudowany w zasilaczu system diagnostyczny do sprawdzenia zasilacza bez konieczności włączania komputera, zasilacz w oferowanym komputerze musi się znajdować na stronie http://www.plugloadsolutions.com/80pluspowersupplies.aspx do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus, w przypadku, kiedy u producenta występuje kilka zasilaczy, które są montowane na etapie produkcji w fabryce załączyć wydruki dla wszystkich zasilaczy. Wydruki 80plus musza być potwierdzone przez producenta lub dołączone oświadczenie producenta

	komputera iż wskazane zasilacze przez wykonawcę spełniają 80plus. Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED np. przycisku POWER [tzn. barw i miganie] W szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wnęk zewnętrznych oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
Bezpieczeństwo	Ukryty w laminacie płyty głównej dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. Zaimplementowany w BIOS lub w menu boot'owania system diagnostyczny z graficznym interfejsem użytkownika, umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System opatrzony min. o funkcjonalność: test procesora, test pamięci, test wentylatora dla procesora, test dysku twardego. System diagnostyczny działający w przypadku braku dysku, uszkodzenia, utraty wszystkich partycji, braku dostępu do internetu, braku dostępu do sieci, bez podłączania zewnętrznych oraz wewnętrznych urządzeń np. pamięć flash USB itp.
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, nazwę producenta komputera, model komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych oraz dodatkowego oprogramowania typu system diagnostyczny odczytania z wewnętrznego menu BIOS informacji o: wersji BIOS, nr seryjnym komputera, dacie wyprodukowania komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej, minimalnej i maksymalnej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, MAC adresie zintegrowanej karty sieciowej, Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Możliwość ustawienia hasła systemowego/użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) oraz uprawniającego do samodzielnej zmiany tego hasła przez użytkownika (bez możliwości zmiany innych parametrów konfiguracji BIOS) przy jednoczesnym zdefiniowanym haśle administratora i/lub zdefiniowanym haśle dla dysku Możliwość wyłączania portów USB w tym: - tylko portów USB znajdujących się na przednim panelu obudowy, - tylko portów USB znajdujących się na tylnym panelu obudowy. - wszystkich portów USB - pojedynczo
Certyfikaty i standardy	Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) Deklaracja zgodności CE (załączyć certyfikat do oferty). Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 (załączyć certyfikat do oferty). Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów

	środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram Komputer musi spełniać wymogi normy Energy Star lub dołączony do oferty certyfikat potwierdzony przez producenta. Wymagany wpis dotyczący oferowanego komputera w internetowym katalogu http://www.energystar.gov – dopuszcza się wydruk ze strony internetowej
Warunki gwarancji	**3-letnia gwarancja producenta świadczona na miejscu u klienta.** Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia Producenta potwierdzonego, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta
Wsparcie techniczne producenta	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony.
System Operacyjny	Zainstalowany system operacyjny Windows 10/11 Professional, klucz licencyjny musi być zapisany trwale w BIOS.
Porty I/O	Wbudowane porty: - panel przedni: 2 x USB 3.2 gen 1, 2 x USB 2.0, 1x audio (dopuszcza się port combo), czytnik kart SD - panel tylny: 1 x audio out, 2 x USB 3.2 gen 1, 2 x USB 2.0, 1 x DisplayPort 1.4, 1 x HDMI 1.4b, 1 x RJ45. Nie dopuszcza się stosowania adapterów, konwerterów, przejściówek w celu uzyskania ww. portów. Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w: 1 x PCI Express x16 Gen.3, 1 x PCI Express x1, min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, min. 2 złącza SATA w tym 1 szt SATA 3.0, 1 złącze M.2 dla dysków SSD, 1 złącze M.2 dla bezprzewodowej karty WiFI. Karta WiFi 5 AC zamontowana w złączu M.2 na płycie głównej.
Wymagania dodatkowe	Klawiatura USB w układzie polski programisty Mysz USB z klawiszami oraz rolką (scroll) Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.
Dodatkowe oprogramowanie	Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające: - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji: a. o poprawkach i usprawnieniach dotyczących aktualizacji b. dacie wydania ostatniej aktualizacji c. priorytecie aktualizacji d. zgodność z systemami operacyjnymi e. jakiego komponentu sprzętu dotyczy aktualizacja f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany

	został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) - sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) - dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.

b) Monitor – 2 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne monitora
Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą IPS 21,5"
Rozmiar plamki (maksymalnie)	0,250 mm x 0,250 mm
Jasność	250 cd/m2
Kontrast	1000:1
Kąty widzenia (pion/poziom)	178/178 stopni
Czas reakcji matrycy (maksymalnie)	5ms (gray to gray) w trybie fast 8ms (gray to gray) w trybie normal
Rozdzielczość maksymalna	1920 x 1080 przy 60Hz
Gama koloru	Min. 99% sRGB
Częstotliwość odświeżania poziomego	30 – 83 kHz
Częstotliwość odświeżania pionowego	56 – 76 Hz
Pochylenie monitora	W zakresie 26 stopni
Wydłużenie w pionie	Tak, min 150 mm
PIVOT	Tak
Obrót lewo/prawo	Min. 90 stopni
Powłoka powierzchni ekranu	Antyodblaskowa
Podświetlenie	System podświetlenia WLED
Zużycie energii	Maksymalne 48W, czuwanie mniej niż 0.2W Energy Star nie więcej niż 12W
Bezpieczeństwo	Monitor musi być wyposażony dedykowany slot na linkę zabezpieczającą
Waga bez podstawy	Maksymalnie 3kg
Waga z podstawą	Maksymalnie 5kg
Złącze	1 x 15-stykowe złącze D-Sub, 1 x HDMI 1.4, 1 x złącze DisplayPort 1.2 4 x USB 3.2 Gen 1 1 x USB 3.2 gen 1 upstream

Gwarancja	**Czas trwania gwarancji min. 3 lata** Czas reakcji serwisu - do końca następnego dnia roboczego Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
Certyfikaty	EPEAT Gold, Energy Star 8.0 Monitor musi się znajdować na stronie TCO: http://tcocertified.com/product-finder/
Inne	Monitor musi posiadać trwałe oznaczenie logo producenta jednostki centralnej. Odłączany stand bez użycia narzędzi VESA 100mm. Mozliwość podłączenia do obudowy dedykowanych głośników

c) <u>All In One – 2 szt.</u>

Nazwa	Wymagane minimalne parametry techniczne
Typ	Komputer stacjonarny. Typu All in One, komputer fabrycznie wbudowany w obudowę monitora. W ofercie wymagane jest podanie modelu producenta komputera.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
Wydajność obliczeniowa	Komputer w oferowanej konfiguracji musi osiągać w teście wydajnościowym Bapco wyniki nie gorsze niż: **SYSmark® 25:** • Overall Rating – co najmniej wynik 1905 punktów • Productivity – co najmniej wynik 1918 punktów • Creativity – co najmniej wynik 1975 punktów • Responsiveness – co najmniej wynik 1670 punktów Dokumentem potwierdzającym spełnianie ww. wymagań będzie dołączony do oferty wydruk raportu z oprogramowania testującego, potwierdzony za zgodność z oryginałem przez Wykonawcę. Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testu Oferent może zostać wezwany do dostarczenia Zamawiającemu oprogramowania testującego, komputera do testów oraz dokładnego opisu metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie wskazanym przez Zamawiającego od momentu otrzymania zawiadomienia.
Wydajność obliczeniowa	Procesor wielordzeniowy osiągający w teście PassMark CPU Mark wynik min. 20290 punktów według wyników ze strony https://www.cpubenchmark.net
Pamięć RAM	8GB DDR4 3200MHz możliwość rozbudowy do 64GB, dwa sloty pamięci, jeden slot wolny
Pamięć masowa	256GB SSD M.2 NVMe Możliwość instalacji dodatkowego dysku twardego 2,5”

Nr referencyjny: IN.271.1.2022

Wydajność grafiki	Grafika zintegrowana z procesorem powinna umożliwiać pracę min. czteromonitorową, współdzielona i dynamicznie przydzielana pamięć z RAM. Oferowany układ graficzny osiągający w teście PassMark Video Cards wynik min. 1630 punktów według wyników ze strony https://www.cpubenchmark.net	
Matryca	Rozmiar matrycy / plamki	min.23,8” / max. 0,275mm
	Rozdzielczość	FHD (1920x1080)
	Jasność typowa	min. 250 cd/m²
	Kontrast typowy	1000:1
	Typowy czas reakcji matrycy	14 ms
	Barwa koloru (typowa)	72% NTSC typowa
	Kąty typowe Horizontal/Vertical	178(+/- 89) / 178 (+/-89)
	Rodzaj matrycy	dotyk pojemnościowy, 10-punktowy multi-touch
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki min. 2W na kanał. Wbudowana w obudowę matrycy cyfrowa kamera o rozdzielczości w podczerwieni min. 0,30 MP z diodą LED informującą użytkownika o pracy, Mechanicznie chowana w obudowie (nie dopuszcza się kamer przekręcanych i wystających poza obrys obudowy)	
Obudowa	Typu All-in-One zintegrowana z monitorem min. 24”. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej, demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi. Komputer musi posiadać możliwość zainstalowania na ścianie przy wykorzystaniu ściennego systemu montażowego VESA 100x100, Suma wymiarów obudowy z zainstalowanym standem nie może przekraczać: 112cm Suma wymiarów obudowy bez zainstalowanego standu nie może przekraczać: 94cm Zasilacz wewnętrzny o mocy min. 160W o efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Zasilacz w oferowanym komputerze musi się znajdować na stronie http://www.plugloadsolutions.com/80pluspowersupplies.aspx, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus Wbudowany w obudowie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System musi zapisywać logi zdarzeń w BIOS. Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz wpisanym na stałe w BIOS. Podstawa jednostki typu All – in – One musi umożliwiać: Regulację pochyłu pionowego w zakresie od -5 do 30 stopni. Regulację wysokości w zakresie minimum 10 cm. Ustawienie jednostki w trybie Pivot. Obrót podstawy w lewą oraz prawą stronę.	
Zgodność z systemami operacyjnymi i standardami	Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera).	
Bezpieczeństwo	Płyta główna zawierająca układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot’owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego jak również pobierania oprogramowania i instalacji na dysku czy w BIOS.	

Dokument należy podpisać kwalifikowanym
podpisem elektronicznym lub podpisem zaufanym
lub elektronicznym podpisem osobistym

	Czujnik otwarcia obudowy, musi zbierać zdarzenia i zapisywać je w BIOS
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu.
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą myszy. (przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury). Pełna obsługa BIOS za pomocą dotyku. (przez pełną obsługę za pomocą dotyku rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez konieczności zmiany tryby w BIOS). Informacje dostępne z poziomu BIOS na potrzeby inwentaryzacji: wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach, procesor (nazwa, typowa prędkość, minimalna, maksymalna, cache L2 i L3) , pojemności zainstalowanego lub zainstalowanych dysków twardych, MAC adres zintegrowanej karty sieciowej, zintegrowany układ graficzny, kontroler audio. Informacje dostępne w samym menu BIOS bez stosowania dodatkowego oprogramowania jak i wbudowanego systemu diagnostycznego. Możliwość, ustawienia hasła na poziomie: - administratora [hasło nadrzędne] umożliwiające logowanie do BIOS, dokonywanie zmian, rozruch komputera, - użytkownika/systemowego [hasło umożliwiające użytkownikowi zmianę swojego hasła, zgodnie z uprawnieniami nadanymi przez administratora dokonywać lub nie zmian ustawień BIOS], rozruch systemu operacyjnego [hasło blokuje start systemu operacyjnego]. - hasło dla dysku Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Możliwość wyłączenia/włączenia karty sieciowej, kontrolera SATA, kontrolera audio, głośników, kamery, mikrofonów, układu TPM, czytnika kart multimedialnych Możliwość włączenia/wyłączenia czujnika otwarcia obudowy, ustawienia go w tryb cichy Możliwość przypisania w BIOS numeru nadawanego przez Administratora oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym. Musi umożliwiać znaki specjalne # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość wyłączania portów USB grupami oraz w szczególności pojedynczo w dowolnej kombinacji. BIOS musi nanosić automatycznie wszystkie zmiany konfiguracji dotyczące w szczególności: pamięci, procesora, dysku.
Certyfikaty i standardy	Certyfikat ISO9001 dla producenta sprzętu (załączyć do oferty) Certyfikat ISO 50001 dla producenta sprzętu Deklaracja zgodności CE (załączyć do oferty) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram Certyfikat TCO - do oferty załączyć certyfikat lub wydruk ze strony http://tcocertified.com/product-finder/
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy jałowej dysku twardego (IDLE) wynosząca maksymalnie 24 dB (załączyć oświadczenie producenta)
System Operacyjny	Zainstalowany system operacyjny Windows 10/11 Professional, klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.
Wymagania	Wbudowane porty:

dodatkowe	Panel tylny : 1x HDMI-IN—HDMI 1.4a 1x HDMI-OUT—HDMI 2.0 1x DisplayPort++ 1.4a/HDCP 2.3 1x RJ45 Ethernet port 2x USB 3.2 Gen 1 typ A z Smart Power On 2x USB 3.2 Gen 2 typ A 1x Line-out audio 1x gniazdo zasilania Panel boczny (nie dopuszcza się portów USB usytuowanych na dolnej krawędzi obudowy z racji na ergonomię pracy a w szczególności regulację wysokości) : 1x SD 4.0 card slot 1x USB 3.2 Gen 2x1 Type-C 1x Uniwersalny audio port (combo) lub 1x port słuchawki i 1 port mikrofon 1x USB 3.2 Gen 1 typ A z PowerShare Wymagane porty USB wbudowane, nie dopuszcza się stosowania rozgałęziaczy, hub'ów itp. Wszystkie porty dostępne dla użytkownika w najniższej możliwej regulacji wysokości Karta sieciowa WiFi 6E z Bluetooth 5.2 Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, min. 1 złącza M.2 2280 dla dysku twardego oraz 1 złącze M.2 karty WiFi Czytnik kart multimedialnych SD 4 Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll)
Dodatkowe oprogramowanie	Oprogramowanie z nieograniczoną czasowo licencją na użytkowanie umożliwiające: - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi - dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji - sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania) - dostęp do wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku *.xml Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku. W ofercie należy podać nazwę oprogramowania
Warunki gwarancji Wsparcie techniczne	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego)

Dokument należy podpisać kwalifikowanym
podpisem elektronicznym lub podpisem zaufanym
lub elektronicznym podpisem osobistym

	3-letnia gwarancja producenta świadczona na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia Producenta potwierdzonego, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta

2. Laptopy – 2 szt.

Nazwa	Wymagane parametry techniczne
Zastosowanie	Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
Matryca	15.6” FHD (1920 x 1080), powłoka przeciwodblaskową, bez dotyku, jasność 250 cd/m2, kontrast 700:1, NTSC 45%
Wydajność	Oferowany komputer przenośny musi osiągać w teście wydajności: **CrossMark:** • Overall Rating – co najmniej wynik 1350 punktów • Productivity – co najmniej wynik 1340 punktów • Creativity – co najmniej wynik 1445 punktów • Responsiveness – co najmniej wynik 1140 punktów Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego.
Procesor	Procesor osiągający w teście PassMark Performance Test, co najmniej 13420 punktów w kategorii Average CPU Mark. Wynik dostępny na stronie: https://www.cpubenchmark.net/cpu_list.php
Pamięć RAM	8GB DDR4 3200MHz możliwość rozbudowy do min. 64GB, nie dopuszcza się pamięci wlutowanych w płytę główną, min. dwa sloty na pamięć
Pamięć masowa	256GB NVMe SSD M.2
Karta graficzna	Wynik karty graficznej w teście PassMark Performance Test co najmniej 2735 punktów w kategorii Average G3D Rating. Dostępny na stronie: http://www.videocardbenchmark.net/gpu_list.php
Klawiatura	Klawiatura w układzie US – QWERTY z wydzieloną klawiaturą numeryczną, z wbudowanym podświetleniem, min 90 klawiszy. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12.
Multimedia	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2x 2W. Kamera internetowa FHD IR 2 Mpix, trwale zainstalowana w obudowie matrycy
Łączność	Karta Wi-Fi 6E AX z transferem do 2400 Mbps + Bluetooth 5.2

bezprzewodowa	
Bateria i zasilanie	**Min. 4-cell [min. 58Whr].** Umożliwiająca jej szybkie naładowanie do 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Zasilacz o mocy min. 90W ze złączem Typu - C
Waga i wymiary	Waga max 1,82kg z baterią 4 cell Suma wymiarów notebooka nie większa niż 615mm mierzona po krawędziach obudowy.
Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka, po zamknięciu przed kurzem i wilgocią. Kąt otwarcia notebooka min 180 stopni. Komputer spełniający normy MIL-STD-810H [załączyć do oferty oświadczenie wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem producenta]
BIOS	BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji, oraz posiadać: datę produkcji komputera (data produkcji nieusuwalna), o kontrolerze audio, procesorze, a w szczególności min. i max. osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne (nieedytowalne) pole asset tag z możliwością wpisywania min. znaków specjalnych. Funkcje logowania się do BIOS na podstawie hasła systemowego/użytkownika, administratora (hasła niezależne), Blokowanie hasłem systemowym/użytkownika rozruch dysku twardego. Funkcja umożliwiająca założenie hasła na dysk, informację o stanie naładowania baterii (stanu użycia), podpiętego zasilacza, zarządzanie trybem ładowania baterii (np. określenie docelowego poziomu naładowania). Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS. Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym.
Certyfikaty	Certyfikat ISO9001 dla producenta sprzętu (należy załączyć do oferty) Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty) Certyfikat ISO 50001 dla producenta sprzętu (należy załączyć do oferty) Certyfikacja TCO dla oferowanego modelu dostępna na stronie https://tcocertified.com/product-finder/ lub załączyć certyfikat do oferty Deklaracja zgodności CE (załączyć do oferty) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony)
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 23dB (załączyć do oferty oświadczenie wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem producenta)
Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. Działający w pełni, bez okrojonych funkcjonalności nawet w przypadku uszkodzonego dysku, braku dysku lub sformatowanym dysku, dostępu do sieci i internetu oraz bez konieczności podłączenia urządzeń wewnętrznych i zewnętrznych oraz bez konieczności pobierania i instalowania np. na ukrytej pamięci flash BIOS
Bezpieczeństwo	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej. Wbudowany czujnik otwarcia obudowy (dolnej pokrywy) Wbudowana w obudowę matrycy technologia IR umożliwiająca autentykację na poziomie oferowanego systemu operacyjnego

Nr referencyjny: IN.271.1.2022

	Czytnik linii papilarnych Czytnik SmartCard
System operacyjny	Zainstalowany system operacyjny Windows 10/11 Professional, klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.
Oprogramowanie dodatkowe	Dołączone do oferowanego komputera oprogramowanie z nieograniczoną licencją czasowo na użytkowanie umożliwiające: - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji: a. o poprawkach i usprawnieniach dotyczących aktualizacji b. dacie wydania ostatniej aktualizacji c. priorytecie aktualizacji d. zgodność z systemami operacyjnymi e. jakiego komponentu sprzętu dotyczy aktualizacja f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga. - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr) - sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania) - dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
Porty i złącza	Wbudowane porty i złącza: 1x HDMI **2.0,** 2x USB 3.2 typ A, 2x Thunderbolt **4**, 1x RJ - 45 [fizyczny port], port audio combo, gniazdo linki zabezpieczającej
Warunki gwarancyjne, wsparcie techniczne	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) **3-letnia gwarancja producenta świadczona na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego.** Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia Producenta potwierdzonego, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta

Dokument należy podpisać kwalifikowanym
podpisem elektronicznym lub podpisem zaufanym
lub elektronicznym podpisem osobistym

Nr referencyjny: IN.271.1.2022

3. Serwery (łącznie 4 szt.)

a) Serwer I – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.8GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 129 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	Minimum 128GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	- minimum trzy sloty PCIe generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT Dodatkowa dwuportowa karta sieciowa 10GbE SFP+
Dyski twarde	Zainstalowane 5 dysków SSD SATA o pojemności min. 960GB, 6Gb, 2,5“ Hot-Plug. Zainstalowane dwa dyski M.2 SATA o pojemności min. 240GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
System operacyjny/System wirtualizacji	Serwerowy system operacyjny Microsoft Windows Serwer 2022: • Licencja serwerowego systemu operacyjnego musi uwzględniać wszystkie rdzenie procesorów zainstalowanych w serwerze. • Licencje serwerowego systemu operacyjnego muszą uprawniać do uruchamiania co najmniej dwóch serwerowych systemów operacyjnych w środowisku wirtualnym. • Licencje serwerowego systemu operacyjnego nie mogą być ograniczone czasowo. • Nośnik CD/DVD • Nośnik do downgrade-u do wersji 2019

Nr referencyjny: IN.271.1.2022

Wbudowane porty	4 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 800W każdy.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw

	sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	**5 lat gwarancji producenta** Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi sie na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowyych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

<u>Wraz z usługą dla zakresu:</u>

- Aktualizacja firmware na serwerze.

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

Nr referencyjny: IN.271.1.2022

- Instalacja hyperwizora VMware ESXi.
- Instalacja Windows Server na wirtualnej maszynie.
- Aktualizacja Windows Server do aktualnej wersji w poprawek.
- Instalacja usługi Secondary DNS.
- Dokumentacja powykonawcza
- Virtualizacja jednego serwera fizycznego - System Debian 4 GNU/Linux - Około 200-300 mb danych
- Przeniesienie 2 maszyn virtualnych VMWare (ESXi 7.0) - łącznie około 1,5 TB danych - obie Oracle Linux 7 64bit
- Konfiguracja backupów wirtualnych maszyn
- Szkolenie z obsługi (4h robocze)

b) Serwer II – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji do 4 dysków 3.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowany jeden procesor 8-rdzeniowy, min. 2.8 GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 127 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.
RAM	32GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	- minimum jeden slot PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 6 interfejsów sieciowych 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Dyski twarde	Zainstalowane 2 dyski SSD SATA o pojemności min. 960GB, 6Gb, 2,5“ Hot-Plug. Zainstalowane dwa dyski M.2 SATA o pojemności min. 240GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde
Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED.
System operacyjny/System wirtualizacji	Serwerowy system operacyjny Microsoft Windows Serwer 2022: • Licencja serwerowego systemu operacyjnego musi uwzględniać wszystkie rdzenie procesorów zainstalowanych w serwerze. • Licencje serwerowego systemu operacyjnego muszą uprawniać do uruchamiania co najmniej dwóch serwerowych systemów operacyjnych w środowisku wirtualnym. • Licencje serwerowego systemu operacyjnego nie mogą być ograniczone czasowo. • Nośnik CD/DVD • Nośnik do downgrade-u do wersji 2019

	• 20 licencji dostępowych User CALs 2022/2019
Wbudowane porty	Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug maksymalnie 600W.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać

	recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	**3 lata gwarancji producenta** Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi sie na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowyych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

c) Serwer III – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji do 4 dysków 3.5" wraz z kompletem szyn umożliwiających montaż w szafie rack.
Płyta główna	Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	Jeden procesor 4-rdzeniowy, min. 2.8GHz (Turbo min. 4.0GHz), umożliwiający osiągnięcie wyniku min. 8000 w teście Average CPU Mark dostępnym na stronie https://www.cpubenchmark.net/.
Pamięć RAM	2x16GB pamięci RAM ECC UDIMM o częstotliwości pracy 2666MT/s. Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024
Wbudowane porty	min. 4 porty USB w tym min. 1 USB 3.0 1 port VGA 1 port RS232
Gniazda PCI	Min. 2 sloty PCIe generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Kontroler dysków	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10
Dyski twarde	Zainstalowane 2 dyski SSD SATA o pojemności min. 960GB, 6Gb, Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Wentylatory	Minimum 3 wentylatory
Zasilacze	Zasilacz o mocy maks. 450W.
System operacyjny/System wirtualizacji	Serwerowy system operacyjny Microsoft Windows Serwer 2022: • Licencja serwerowego systemu operacyjnego musi uwzględniać wszystkie rdzenie procesorów zainstalowanych w serwerze. • Licencje serwerowego systemu operacyjnego muszą uprawniać do uruchamiania co najmniej dwóch serwerowych systemów operacyjnych w środowisku wirtualnym. • Licencje serwerowego systemu operacyjnego nie mogą być ograniczone czasowo. • Nośnik CD/DVD • Nośnik do downgrade-u do wersji 2019 • 15 licencji dostępowych User CALs 2022/2019
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła

	• Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows

	Server 2019, Microsoft Windows Server 2022.
Warunki gwarancji	**3 lata gwarancji producenta**, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

d) Oprogramowaniem do wirtualizacji (1 licencja) – wymagania minimalne:

1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
3. Pojedynczy klaster może się skalować do 3 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
4. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB.
5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia 24 TB pamięci operacyjnej RAM.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.
8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 20 portów USB.
9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 4 GB pamięci graficznej.
10. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
11. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
12. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7/8/10, Windows Server, Amazon Linux 2, macOS, OS X, Asianux, Ubuntu, CentOS, NeoKylin, CoreOS, Debian, FreeBSD, Oracle Linux, RHEL, SUSE, Photon OS.

13. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
14. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
15. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
16. System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
17. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
18. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
19. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Wsparcie techniczne musi być świadczone bezpośrednio przez producenta oprogramowania. Licencjonowanie nie może odbywać się w trybie OEM.
20. Rozwiązanie musi zawierać zintegrowaną funkcjonalność do zarządzania poprawkami i podnoszenia wersji wirtualizatora.
21. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
22. Oprogramowanie do wirtualizacji musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
23. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
24. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna dostarczana jest w postaci gotowej, wstępnie skonfigurowanej maszyny wirtualnej tzw. virtual appliance. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem protokołu HTML5.
25. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane historyczne.

e) Serwer IV– 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji do 4 dysków 3.5" wraz z kompletem szyn umożliwiających montaż w szafie rack.
Płyta główna	Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	Jeden procesor 4-rdzeniowy, min. 2.8GHz (Turbo min. 4.0GHz), umożliwiający osiągnięcie wyniku min. 8000 w teście Average CPU Mark dostępnym na stronie https://www.cpubenchmark.net/.
Pamięć RAM	2x16GB pamięci RAM ECC UDIMM o częstotliwości pracy 2666MT/s. Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024
Wbudowane porty	min. 4 porty USB w tym min. 1 USB 3.0

	1 port VGA 1 port RS232
Gniazda PCI	Min. 2 sloty PCIe generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Kontroler dysków	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10
Dyski twarde	Zainstalowane 2 dyski SSD SATA o pojemności min. 960GB, 6Gb, Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Wentylatory	Minimum 3 wentylatory
Zasilacze	Zasilacz o mocy maks. 450W.
System operacyjny/System wirtualizacji	Serwerowy system operacyjny Microsoft Windows Serwer 2022: • Licencja serwerowego systemu operacyjnego musi uwzględniać wszystkie rdzenie procesorów zainstalowanych w serwerze. • Licencje serwerowego systemu operacyjnego muszą uprawniać do uruchamiania co najmniej dwóch serwerowych systemów operacyjnych w środowisku wirtualnym. • Licencje serwerowego systemu operacyjnego nie mogą być ograniczone czasowo. • Nośnik CD/DVD • Nośnik do downgrade-u do wersji 2019 • 5 licencji dostępowych User CALs 2022/2019
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;

	• możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	**3 lata gwarancji producenta** Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi sie na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.

	Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowyych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

4. UPS – 1 szt.

Wymagania minimalne:

- MOC min. - 1500VA/1500W
- Obudowa – Rack , max. 2U
- Topologia – Line-interactive
- Kształt napięcia w trybie bateryjnym - Czyste napięcie sinusoidalne
- Czas przełączania – do 4ms
- Czas ładowania akumulatorów – do 3 godzin
- Czas podtrzymania dla obciążenia 1000 W– min 11 min.
- Ilość gniazd wyjściowych - co najmniej 10 (UPS musi posiadać wydzieloną grupę gniazd dla obciążeń kluczowych/krytycznych oraz dla pozostałych obciążeń)
- Porty komunikacyjne: USB, RS232, EPO, Dry contact
- Komunikacja po protokole SNMP/HTTP – TAK
- Oprogramowanie do zarządzania UPSem z możliwością współpracy ze środowiskiem VMware ESXi 7.0
- Rozproszenie ciepła online (BTU/h) – do 80 BTU/h
- **Gwarancja – 2 lata**

5. Skanery dokumentów – 3 szt.

Minimalne wymagania Techniczne	
Parametr	**Opis funkcjonalny**
Typ skanera (obudowa)	Kompaktowy skaner A4 z automatycznym podajnikiem dokumentów (ADF)

Nr referencyjny: IN.271.1.2022

Sposoby skanowania	Skanowanie jednostronne Skanowanie dwustronne w jednym przebiegu Prosta ścieżka podawania papieru zapewniająca prawidłowe układanie dokumentów po zeskanowaniu na tacy odbiornika
Automatyczny podajnik dokumentów (ADF)	O pojemności co najmniej 100 arkuszy A4 (80 g/m^2) z możliwością regulacji bocznych prowadnic podajnika
Obsługiwane formaty (nie złożone na pół)	Minimum w zakresie A4, A5, A6, B5, B6 Minimalny rozmiar: 50 x 50 mm Maksymalny rozmiar: 216 x 355 mm
Obsługa długich dokumentów	do 6 m
Gramatura obsługiwanych dokumentów w trybie podawania automatycznego bez korzystania z dodatkowych akcesoriów	20 – 460 g/m^2
Obsługa niestandardowych nośników	Karty plastikowe oraz ID do grubości 1.4mm (w tym tłoczone), paszporty oraz broszury do grubości 5 mm (np. paszport)
Detekcja podwójnych pobrań	Co najmniej jeden czujnik ultradźwiękowy z funkcją automatycznego zachowania obrazu dla umyślnie nałożonych obiektów (takich jak przyklejone notatki lub przymocowane taśmą paragony) zgodnie z ustawionym wzorcem
Ochrona skanowanych dokumentów	Ochrona dokumentów w oparciu o detekcję przekosu obrazu.
Szybkość skanowania (dla dokumentów A4 przy 200 oraz 300 dpi w trybach mono i kolor)	Minimum 45 arkuszy/min., 100 obrazów/min
Typowe dzienne obciążenie skanera	minimum do 7 500 arkuszy (kartek)
Układ optyczny (przetwornik obrazu)	Wykonany w technologii CCD (Charge Coupled Device) lub CIS (Contact Image Sensor) – minimum przetwornik w skanerze ADF - 1 z przodu, 1 z tyłu
Optyczna rozdzielczość skanowania	optyczna 600 dpi, sterownik 1200 dpi
Wyjściowa rozdzielczość skanowania	60-600 dpi z możliwością skokowej regulacji co 1 dpi
Tryby koloru skanowania	Monochromatyczny, odcienie szarości, kolor
Obsługiwane systemy operacyjne	Windows 7/8.1/10/11
Interfejsy komunikacyjne	Minimum USB 3.2 Gen 1 oraz Ethernet 10BASE-T/100BASE-TX/1000BASE-T (wszystkie interfejsy fabrycznie zintegrowane w urządzeniu)
Obsługiwane sterowniki	Zgodne ze standardem TWAIN oraz ISIS

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

Nr referencyjny: IN.271.1.2022

Funkcje poprawy jakości skanów	Obsługa poniższych funkcjonalności dla zarówno dla standardu TWAIN oraz ISIS: 1) automatyczna poprawa jakości skanowanych dokumentów 2) automatyczne prostowanie i orientacja obrazu 3) automatyczne przycinanie do oryginalnego rozmiaru dokumentu 4) automatyczne usuwanie niezadrukowanych stron 5) automatyczna detekcja koloru 6) automatyczna naprawa uszkodzonych lub zagiętych krawędzi dokumentu 7) interaktywna regulacja koloru, jasności i kontrastu bez konieczności ponownego skanowania 8) skanowanie wielostrumieniowe w jednym przebiegu z możliwością wyboru dowolnej kombinacji trybów koloru 9) łączenie i dzielenie obrazów 10) redukcja pionowych smug powstających na wskutek zabrudzenia 11) wypełnianie otworów w obrazie
Funkcje dołączonego oprogramowania obsługującego standardy TWAIN oraz ISIS	Detekcja i separacja na podstawie kodów kreskowych typu 3z9, ITF, EAN128, NW7, separacja dokumentów za pomocą niezadrukowanej kartki, odczytaną wartością ze strefy OCR, tzw. "patch code" (typ 1, 2, 3, 4, T) oraz na podstawie układu formularza. Automatyczne nazewnictwo plików za pomocą kodów kreskowych i wartości odczytanej ze strefy OCR z tworzeniem wielopoziomowej struktury katalogów. Podświetlanie pustych stron i sygnalizacja obrazów o niepewnej jakości w interfejsie użytkownika. Obsługiwane formaty plików wyjściowych PDF, PDF/A, PDF przeszukiwalny, JPEG, JPEG2000, XLSX, DOCX, PPTX, TIFF, MTIFF, PNG, BMP. Zapis plików wyjściowych dla poszczególnych strumieni obrazu do oddzielnych folderów na dysku z możliwością wyboru różnych rozszerzeń (formatów) plików, automatyczny odczyt informacji ze stref MRZ dla paszportów oraz dowodów osobistych i zapis do metadanych w formatach XML lub CSV. Skanowanie bez konieczności podłączania skanera do lokalnej stacji roboczej i instalacji sterowników
Funkcje dołączonego oprogramowania do zarządzania i monitoringu	Działające w strukturze klient-serwer (dwukierunkowa komunikacja wyłącznie w obrębie lokalnej sieci LAN) umożliwiające scentralizowane zarządzanie i monitoring oferowanych skanerów w tym: zdalna aktualizacja sterowników, oprogramowania sprzętowego (firmware) i zdalna konfiguracja ustawień skanerów (na wielu stacjach jednocześnie), generowanie alertów o stanie skanera (błędy) i potrzebie wymiany elementów eksploatacyjnych.
Ergonomia pracy	Skaner ważący nie więcej niż 3.6 kg o powierzchni podstawy urządzenia mniejszej niż 0,052m^2 Możliwość obsługi procesu skanowania z przycisków znajdujących się na skanerze. Maksymalny pobór mocy w trybie pracy mniejszy niż 22 W. Możliwość integracji skanera z modułem drukującym realizującym automatyczny nadruk daty skanowania dokumentu po zeskanowaniu
Materiały eksploatacyjne	Materiały eksploatacyjne zainstalowane w skanerze pozwalające na zeskanowanie do 200 000 arkuszy
Normy i regulacje	Urządzenie posiada oznakowanie CE potwierdzające zgodność z wymaganiami UE nałożonymi na producenta, spełniające kryteria Energy Star oraz RoHS

Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub elektronicznym podpisem osobistym

Gwarancja	**36 miesięcy**

6. Monitor – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne monitora
Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą IPS 49”
Rozmiar plamki (maksymalnie)	0,234 mm x 0,234 mm
Jasność	350 cd/m²
Zaokrąglony ekran	Tak (3800R)
Kontrast	1000:1
Kąty widzenia (pion/poziom)	178/178 stopni
Czas reakcji matrycy (maksymalnie)	8 ms (normalny); 5 ms (szybki) - (gray to gray)
Rozdzielczość maksymalna	5120 x 1440 przy 60 Hz
Gama koloru	Min. 99% sRGB
Współczynnik kształtu	32:9
Pochylenie monitora	-5/+21
Regulacja wysokości	Tak, min 90 mm
PbP	Tak
Obrót lewo/prawo	-170 do 170 stopni
Powłoka powierzchni ekranu	Antyrefleksyjny, 3H Hard Coating
Podświetlenie	System podświetlenia WLED
Zużycie energii	Typowo 60W, maksymalnie 230W, czuwanie mniej niż 0.5W
Bezpieczeństwo	Monitor musi być wyposażony dedykowany slot na linkę zabezpieczającą
Waga bez podstawy	Maksymalnie 11,4kg
Waga z podstawą	Maksymalnie 17,2 kg
Złącze	• 2 x HDMI • DisplayPort • 2 x USB 3.0 — upstream • 5 x USB 3.0 — downstream • USB-C
Wbudowane urządzenia	Koncentrator USB 3.0
Wymiary (szer./głęb./wys.)	121.51 cm x 25.26 cm x 45.86 cm - z podstawką

Gwarancja	**Czas trwania gwarancji min. 3 lata** z opcją zaawansowanej wymiany w przypadku "jasnych pikseli". Czas reakcji serwisu - do końca następnego dnia roboczego Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
Certyfikaty	EPEAT Gold, Energy Star 8.0 Monitor musi się znajdować na stronie TCO: http://tcocertified.com/product-finder/
Inne	Monitor musi posiadać trwałe oznaczenie logo producenta jednostki centralnej. Odłączany stand bez użycia narzędzi VESA 100mm.

7. Serwery plików (łącznie 3 szt.)

a) Serwer plików I – 1 szt.

Minimalne wymagania Techniczne	
Parametr	**Opis funkcjonalny**
Procesor	Czterordzeniowy procesor Intel Celeron J4125 2,0GHz z przyspieszeniem do 2,7GHz
Obudowa	Tower o wymiarach 166 × 199 × 223 mm
Pamięć RAM	Pamięć 8 GB DDR4 SO-DIMM
Ilość obsługiwanych dysków	4 dysków o maksymalnej pojemności 16TB każdy, po podłączeniu modułu rozszerzającego 9 dysków; 2 dyski M.2 2280 NVMe SSD
Ilość zainstalowanych dysków	2 dyski HDD o pojemności min 2TB znajdujących się na liście zgodności producenta serwera NAS; wsparcie producenta dysku w odzyskiwaniu danych z dysku w przypadku uszkodzenia
Interfejsy sieciowe	2 x Gigabit (10/100/1000); Wsparcie dla Link Agregation.
Porty	2 x USB3.2 gen 1 1 x eSATA
Wskaźniki LED	Status, HDD1-4, Power on
Obsługa RAID	Basic, JBOD, RAID 0,1,5,6,10, SHR + Obsługa Hot Spare dla SHR,RAID 1,5,6 (z dodatkową jednostką rozszerzającą), 10 (z dodatkową jednostką rozszerzającą),
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Szyfrowanie	Możliwość szyfrowania wybranych udziałów sieciowych.
System Operacyjny	Windows 7 i 10, Mac OS X 10.11 i nowsze
Licencja na Kamery IP	W zestawie licencja na dwie kamery z możliwością rozszerzenia do 40.
Protokoły	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP)
Usługi	Serwer VPN Serwer pocztowy dla kilku domen Stacja monitoringu Windows ACL Integracja z Windows ADS Firewall

	Serwer WWW Serwer plików Manager plików przez WWW Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie Usługa DDNS Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID Snapshot Replication Oprogramownie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji VMware Wsparcie dla High Availability
Obsługa migawek	• Maksymalna liczba migawek folderów współdzielonych: 1 024 • Maksymalna liczba migawek systemu: 65 536
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów
Język GUI	Polski
Gwarancja i serwis	**3 lat gwarancji**
Waga	Max. 2,3 kg
Certyfikaty	EAC, VCCI, CCC, RCM, KC, FCC, CE, BSMI
System plików	Dyski wewnętrzne Btrfs EXT4. Dyski zewnętrzne Btrfs, FAT, NTFS, EXT3, EXT4, HFS+, exFAT*(z dodatkową licencją)
Szyfrowanie	Mechanizm szyfrowania sprzętowego (AES-NI)
Liczba wolumenów	Do 64
Liczba iSCSI Targetów	Do 128
Liczba iSCSI LUN	Do 256
Liczba kont użytkowników	2048
Liczba grup	256
Liczba folderów udostępnionych	512
Ilość jednoczesnych połączeń	1000 dla CIFS/AFP/NFS/FTP/WebDAV
Maks. liczba kamer IP	Obsługa do 40 kamer w tym 2 licencje darmowe
Zasilacz	100W
Chłodzenie	FAN x 2 92 x 92 mm

b) Serwer plików II – 2 szt.

Minimalne wymagania Techniczne	
Parametr	**Opis funkcjonalny**
Procesor	Czterordzeniowy procesor AMD Ryzen™ V1500B (8-wątkowy) 2,2 GHz
Obudowa	Rack 1U o wymiarach 44 × 430,5 × 457,6 mm/44 × 480 × 492,6 mm (z uchwytami serwera); szyny teleskopowe do instalacji w szafie RACK
Pamięć RAM	Pamięć 2 GB DDR4 ECC SODIMM (z możliwością rozszerzenia do 32 GB)
Ilość obsługiwanych dysków	4 dysków 3,5" lub 2,5" SATA HDD/SSD z możliwością podłączenia półki rozszerzającej o 4 dyski
Ilość zainstalowanych dysków	2 dyski HDD o pojemności min 4TB znajdujących się na liście zgodności producenta serwera NAS; wsparcie producenta dysku w odzyskiwaniu danych z dysku w przypadku uszkodzenia
Interfejsy sieciowe	4 porty 1GbE RJ-45
Porty	2 porty USB 3.2 1. generacji 1 gniazdo rozszerzenia (eSATA) 1x PCIe 4-liniowe gniazdo x8 generacji 3

Wskaźniki LED	Zasilanie, alert, status, LAN, HDD1-4
Obsługa RAID	Synology Hybrid RAID (SHR), Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6 i RAID 10
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Licencja na Kamery IP	W zestawie dwie licencje na jedną kamerę z możliwością rozszerzenia do 40.
Protokoły	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP i VPN (PPTP, OpenVPN™, L2TP)
Usługi	Wsparcie dla High Availability Serwer VPN Serwer pocztowy dla kilku domen Stacja monitoringu Windows ACL Integracja z Windows ADS Firewall z kontrolą ruchu Serwer WWW Serwer plików Manager plików przez WWW Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie Antyvirus Klient VPN Usługa DDNS Oprogramownie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji VMware
Obsługa migawek	• Maksymalna liczba migawek na foldery współdzielone: 1 024 • Maksymalna liczba migawek systemu: 65 536
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów,
Język GUI	Polski
Gwarancja i serwis	**3 lata gwarancji**
Waga	6,4 KG
Certyfikaty	CE
System plików	Wewnętrzny: Btrfs, ext4 Zewnętrzny: Btrfs, ext4, ext3, FAT32, NTFS, HFS+, exFAT
Liczba wolumenów	Do 64
Liczba iSCSI Targetów	Do 128
Liczba iSCSI LUN	Do 256
Liczba kont użytkowników	2048
Liczba grup	256
Liczba udziałów	512
Ilość jednoczesnych połączeń	500 dla CIFS/AFP/NFS/FTP/WebDAV; 2,000 po rozszerzeniu RAM
Chłodzenie	FAN x 3 40 x 40 mm

7. Zakup i wdrożenie centralnej platformy e-Usług mieszkańca wraz z dokupieniem modułu do systemu dziedzinowego

a) Centralna Platforma e-Usług Mieszkańca – 1 szt.

Efektem realizacji tego zadania będzie uruchomienie Platformy e-Usług zasilonej następującymi e-Usługami z systemu dziedzinowego Respons Urzędu Miejskiego w Sędziszowie:

Nr referencyjny: IN.271.1.2022

1) Informacja – Podatek od nieruchomości (minimum 4 Poziom Dojrzałości - dalej PD)
2) Informacja – Podatek rolny (min. 4 PD)
3) Informacja – Podatek leśny (min. 4 PD)
4) Deklaracja – podatek od nieruchomości (min. 4 PD)
5) Deklaracja – podatek rolny (min. 4 PD)
6) Deklaracja – podatek leśny (min. 4 PD)
7) Deklaracja – środki transportu (min. 4 PD)
8) Deklaracja – odpady komunalne (min. 4 PD)
9) Pismo ogólne (min. 3 PD)
10) Wnioskiem o dopisanie wyborcy do rejestru wyborców drogą elektroniczną, uzyskanie urzędowego potwierdzenia przedłożenia, uzyskanie elektronicznej decyzji o dopisaniu wyborcy do rejestru wyborców.

Platforma eUsług Mieszkańca

Platforma eUsług Mieszkańca to platforma integrujący wszystkie dane z innych systemów, informacje o świadczonych e-usługach przez ePUAP, spersonalizowane dane podatkowe. Jest to główny system funkcjonalny z punktu widzenia mieszkańca działający na styku Klient - Urząd. Dzięki niemu mieszkańcy będą mieli dostęp do wszystkich produktów wytworzonych w ramach projektu. W szczególności system zawierać powinien:
1. opisy wszystkich świadczonych przez urząd e-usług – w tym również na platformie ePUAP, z których mieszkaniec może skorzystać w sposób elektroniczny;
2. posiadać możliwość śledzenia postępu swoich spraw;
3. umożliwiać podgląd swoich, spersonalizowanych danych o należnościach i zobowiązaniach z tytułu podatków i opłat lokalnych;
4. zapewniać możliwość dokonania płatności z tytułu podatków i opłat lokalnych;
5. udostępniać możliwość umówienia się na wizytę w Urzędzie. Mieszkaniec może przejrzeć dyżury i umówić się na spotkanie w urzędzie.

<u>Wymagania ogólne Platformy eUsług Mieszkańca</u>

1. System musi być zbudowany i wdrożony zgodnie z obowiązującymi przepisami prawa, zgodnie z strukturą organizacyjną i regulaminem urzędu oraz dobrymi praktykami funkcjonującymi w JST.
2. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień jego instalacji (tzn. powinno być dostosowane do zmieniających się powszechnie obowiązujących przepisów prawa lub regulacji wewnętrznych Zamawiającego).
3. System musi umożliwiać definiowanie dowolnej ilości użytkowników.
4. System musi być w całości spolonizowany, a więc posiadać polskie znaki i instrukcję obsługi po polsku dla użytkownika oraz administratora. System przygotowany jest do obsługi innych języków, ale do tego potrzebne jest wskazanie jakie mają to być języki oraz wsparcie tłumacza.
5. System musi posiadać jednolity graficzny interfejs użytkownika gwarantujący wygodne wprowadzanie danych, przejrzystość prezentowania danych na ekranie oraz wygodny sposób wyszukiwania danych po ergonomicznie dobranych kryteriach.
6. System musi gwarantować integralność danych, bieżącą kontrolę poprawności wprowadzanych danych, spójność danych (zapewnia to baza danych PostgreSQL).
7. System musi pracować w środowisku sieciowym i posiadać wielodostępność pozwalającą na równoczesne korzystanie z bazy danych przez wielu użytkowników.
8. System musi gwarantować możliwość wdrożenia integracji z Systemami Dziedzinowymi (dalej SD) oraz innymi Systemami. Za integrację odpowiada szyna danych WSO2 ESB.
9. System musi posiadać mechanizmy umożliwiające weryfikację integralności danych tj. identyfikację użytkownika i ustalenie daty wprowadzenia i modyfikacji danych. W znacznym stopniu za identyfikację wykonanych czynności odpowiada dziennik zdarzeń.
10. System musi posiadać mechanizmy ochrony danych przed niepowołanym dostępem, nadawania uprawnień dla użytkowników do korzystania z modułów jak również do korzystania z wybranych funkcji. System jest oparty o mechanizm ról i uprawnień.

11. System dostarczany w ramach projektu nie mogą być przeznaczone przez producenta do wycofania z produkcji, sprzedaży lub wsparcia technicznego
12. Dostarczone oprogramowanie musi być oprogramowaniem w wersji aktualnej.
Dla dostarczonego oprogramowania należy dostarczyć: licencje, nośniki instalacyjne, instrukcje użytkownika i administratora (w formie elektronicznej).

Wymagania funkcjonalne Platformy eUsług Mieszkańca
1. Platforma musi umożliwiać bezpieczne zalogowanie się przez przeglądarkę z wykorzystaniem SSO (Single Sign-On) z wykorzystanie usługi Krajowego Węzła Europejskiej Sieci Indentyfikacji Elektronicznej – w skrócie „Węzła Krajowego" lub „login.gov.pl
2. Platforma musi umożliwiać pozyskiwanie z Systemu Dziedzinowego danych o aktualnych zobowiązaniach zalogowanego interesanta z uwzględnieniem należności dodatkowych tj. odsetki i inne koszty na bieżącą datę logowania w zakresie:
- prowadzenia spraw w zakresie podatku od nieruchomości od osób fizycznych,
- prowadzenia spraw w zakresie podatku od nieruchomości od osób prawnych,
- prowadzenia spraw w zakresie podatku rolnego od osób fizycznych,
- prowadzenia spraw w zakresie podatku rolnego od osób prawnych,
- prowadzenia spraw w zakresie podatku leśnego od osób fizycznych,
- prowadzenia spraw w zakresie podatku leśnego od osób prawnych,
- prowadzenia spraw w zakresie podatku od środków transportowych.
- prowadzenia spraw w zakresie opłaty za gospodarowanie odpadami.
- prowadzenie spraw w zakresie opłat za wodę i ścieki
3. Platforma musi zawierać elektroniczne biuro interesanta stanowiące wirtualny punkt przyjęć formularzy elektronicznych stosowanych w urzędzie oraz informacji dotyczących sposobu załatwienia spraw, co najmniej w zakresie odpowiadającym e-usługom wdrażanym w ramach zamówienia.
4. Platforma w części publicznej musi prezentować skategoryzowane karty usług.
5. Platforma musi być podzielna na część publiczną – udostępnianą niezalogowanym użytkownikom i użytkownikom zalogowanym do platformy oraz część wewnętrzną – dla administratora systemu i pracowników urzędu.
6. Użytkownik w części publicznej powinien mieć możliwość przejrzenia karty usługi, dla której prezentowanej jest opis zredagowany przez administratora oraz możliwość przejścia do wypełnienia formularza elektronicznego na ePUAP.
7. Karta usługi powinna być charakteryzowana przynajmniej przez następujące atrybuty: nazwę, opis, do kogo jest skierowana (obywatel - czyli usługi typu A2C, przedsiębiorcy - czyli usługi typu A2B, instytucji/urzędu – czyli usługi typu A2A).
8. Administrator musi mieć możliwość zdefiniowania karty usługi i utworzenia jej wizualizacji.
9. Platforma musi umożliwiać zarządzanie rejestrem interesantów, gdzie każdego interesanta można:
- zidentyfikować minimum takimi danymi jak: typ podmiotu, imię, nazwisko, login, dane kontaktowe (telefon, email, faks, www, adres korespondencyjny, oraz dowolną liczbę innych form kontaktu),
- zmienić mu dane podstawowe,
- zmienić mu dane kontaktowe,
- powiązać go z interesantem z Systemu Dziedzinowego,
- aktywować konto interesanta,
- przypisać interesanta do grup użytkowników.
10. Administrator musi mieć możliwość powiązania użytkownika z jednym lub kilkoma kontami kontrahenta w Systemie Dziedzinowym. Powiązywanie z kontrahentami SD polega na potwierdzaniu tożsamości interesanta i wprowadzeniu jego numeru PESEL (lub NIP). Jeśli w SD kontrahenci są przypisani do danego numeru PESEL (lub NIP), to pobierane będą dane wszystkich tych kontrahentów. W przypadku zalogowania się do platformy za pośrednictwem Węzła Krajowego (login.gov.pl) potwierdzenie tożsamości następuje automatycznie.
11. Użytkownik zalogowany do Platformy musi mieć możliwość przeglądania i zmiany własnych danych: typ podmiotu (osoba fizyczna / osoba prawna), imię, nazwisko / nazwa, dane kontaktowe standardowe: telefon, email, fax, www, adres korespondencyjny, dane kontaktowe dodatkowe.

12. Użytkownik musi mieć możliwość zmiany hasła oraz ponownego jego nadania w przypadku zagubienia hasła.
13. Użytkownik musi mieć możliwość powiązania konta z kontem ePUAP. Powiązanie następuje poprzez przypięcie numeru PESEL do danego konta interesanta. Jeśli interesant zaloguje się za pomocą Węzła Krajowego (login.gov.pl), to zostanie automatycznie zalogowany na konto jeśli jego numer PESEL jest powiązany z interesantem.
14. Użytkownik musi mieć możliwość odłączenia konta od ePUAP. Odłączanie polega na wycofaniu potwierdzenia tożsamości poprzez usunięcie numeru PESEL przypisanego do konta interesanta.
15. Użytkownik musi mieć możliwość przeglądu swoich danych kontrahenta z Systemu Dziedzinowego, o ile jego konto zostało powiązane z kontem kontrahenta Systemu Dziedzinowego.
16. Dane podstawowe prezentowane w przypadku powiązania konta z kontrahentem Systemu Dziedzinowego to co najmniej: nazwisko imię / nazwa, typ, PESEL, NIP, data wyrejestrowania lub zgonu (jeśli widnienie w Systemie Dziedzinowym).
17. O ile konto interesanta ma potwierdzoną tożsamość to system prezentuje dla danego użytkownika:
- dane adresowe, o ile użytkownik jest zameldowany na terenie Gminy (System Dziedzinowy),
- listę nieruchomości, gdzie dla każdej nieruchomości prezentowana jest wielkość, typ nieruchomości, typ własności oraz lista opłat i podatków pobieranych z tytułu nieruchomości: m.in.: podatek od osób fizycznych, podatek od osób prawnych (System Dziedzinowy),
- listę środków transportu – podlegającą opłatom o ile w Systemie Dziedzinowym użytkownik jest podmiotem prawnym posiadającym opodatkowane środki transportu (System Dziedzinowy),
- listę dokumentów z rozdzieleniem na dokumenty wpływające do urzędu oraz wychodzące z urzędu dla zalogowanego użytkownika w zakresie e-usług,
- listę opłat lokalnych (skarbowe, opłaty dot. zajęcia pasa drogowego, koncesje alkoholowe oraz inne opłaty) (System Dziedzinowy),
- listę faktur do zapłaty o ile dotyczy (System Dziedzinowy).
18. Po zalogowaniu na swoje konto interesant musi mieć możliwość wyświetlenia informacji o wszystkich swoich należnościach wobec Urzędu pobranych z Systemu Dziedzinowego oraz historię swoich płatności. Platforma musi umożliwiać przegląd wszystkich zobowiązań finansowych z uwzględnieniem tytułu należności, należności głównej, odsetek, kosztów upomnień, wezwań do zapłaty, salda do zapłaty, terminie płatności, kwocie już zapłaconej (w przypadku należności, która została już częściowo spłacona), kwocie zleconej płatności poprzez platformę oraz dacie i godzinie zlecenia tej płatności.
19. Należność zawiera co najmniej (jeśli dotyczy) takie informacje jak: numer decyzji, naliczone odsetki oraz koszty upomnień i wezwań, czy był na nią wystawiony tytuł wykonawczy itp.
20. Możliwość prezentowania i wyszukiwania konkretnej należności według rodzaju, daty, terminu płatności itp.
21. Jeżeli należność została dopiero częściowo spłacona to użytkownik musi mieć możliwość otrzymania pełnej informacji w układzie: saldo do zapłaty, ile było wpłat na daną należność, kwota każdej płatności, data płatności oraz informację czy płatność została już zaksięgowana czy nie.
22. Możliwość wyświetlania historii wszystkich interakcji finansowych mieszkańca z urzędem, jakie zostały zrealizowane poprzez system.
23. Dostarczona platforma powinna być zintegrowana z najpopularniejszymi systemami płatniczymi, co najmniej PayByNet (KIR), Przelewy 24, BlueMedia.
24. Platforma musi pozwalać na wnoszenie opłat za pośrednictwem systemu płatności elektronicznych w różny sposób tzn. przez wygenerowanie płatności na wybraną należność i opłacenie, lub na zaznaczenie kilku należności i zapłacenie je jednym przelewem.
25. Możliwość ustawienia sortowania wyświetlanych danych rosnąco lub malejąco względem dowolnego z wyświetlanych parametrów należności.
26. Jeśli należność jest płatna w ratach (np. należności podatkowe, należności rozłożone przez Urząd na raty) platforma powinna również przedstawiać klientowi informację, którą ratę kwota płatności stanowi.
27. W sytuacji, kiedy kilku klientów jest solidarnie zobowiązanych do zapłaty należności klient zalogowany do platformy musi widzieć również minimum imię, nazwisko i adres pozostałych współzobowiązanych. W przypadku podmiotów gospodarczych będzie to nazwa firmy i jej siedziba.

28. W przypadku, jeśli należność powstała w drodze decyzji administracyjnej Urzędu numer decyzji ma być również widoczny dla klienta.
29. Możliwość ukrycia wyświetlania wybranych parametrów należności wyszukiwanych na ekranie użytkownika.
30. System powinien posiadać mechanizmy kontroli i bezpieczeństwa chroniące użytkowników przed kilkukrotnym wniesieniem płatności z tego samego tytułu.
31. Platforma musi generować komunikaty informujące i/lub ostrzeżenia wizualne dla użytkownika podczas próby ponownego zlecenia płatności dla należności, dla których płatność została zlecona za pośrednictwem platformy, a transakcja jeszcze jest przetwarzana.
32. Możliwość wydrukowania wypełnionego polecenia przelewu bankowego lub pocztowego, dla zaznaczonej jednej lub zaznaczonych wielu należności.
33. Możliwość wyszukiwania i prezentowania należności według jej rodzaju, czy statusu płatności tzn. np. pokaż tylko zaległe itp.
34. Możliwość wysyłania informacji o terminie płatności za pośrednictwem SMS.
35. Wygenerowane płatności zlecone za pośrednictwem platformy, ale jeszcze niezaksięgowane powinny zawierać informacje takie jak: nr konta bankowego, kwota i data zlecenia, status zlecenia oraz data wykonania.
36. Informacje o wygenerowanych płatnościach muszą być przesyłane z platformy do Systemu Dziedzinowego. Proces przesyłania danych musi mieć możliwość ustawienia częstotliwości wykonana dla administratora systemu.
37. Możliwość wyszukiwania lub filtrowania poleceń płatności według co najmniej: konta bankowego, rodzaju należności, kwoty, typu płatności, stanu zlecenia, daty zlecenia.
38. Możliwość przeglądu operacji księgowych już zrealizowanych tzn. opłaconych (wpłaty, zwroty, przeksięgowania).
39. Przegląd poleceń przelewów już zrealizowanych na należnościach z wyszczególnionym dla każdej operacji co najmniej: jej rodzajem, kontem bankowym, na którym została zaksięgowana operacja, identyfikatorem, kwotą zapłacona faktycznie, datą i godziną przelewu.
40. Możliwość ustawienia sortowania wyświetlanych danych rosnąco lub malejąco względem dowolnego z wyświetlanych parametrów.
41. Możliwość wyszukiwania lub filtrowania w toku oraz zrealizowanych poleceń przelewów według co najmniej: statusu zlecenia, koncie mieszkańca z platformy, tytule przelewu, koncie bankowym, kwocie płatności od-do, typie płatności.
42. Dla należności dotyczących nieruchomości system musi prezentować dodatkowo minimum: numer decyzji, typ nieruchomości, numer nieruchomości, numer dokumentu własności/władania, datę wydania dokumentu – pobrane z Systemu Dziedzinowego.
43. Dla należności dotyczących podatku od osób prawnych system musi prezentować dodatkowo rok wydania decyzji, typ dokumentu, rodzaj podatku.
Dla danych upomnienia system musi prezentować dodatkowo: numer upomnienia, rok upomnienia, koszt upomnienia, datę wydania upomnienia, datę odbioru upomnienia, kwotę do zapłaty.
44. Platforma musi być przystosowany do obsługi przez osoby niepełnosprawne, tj. musi spełniać wymogi co najmniej WCAG 2.1.

<u>Wymagania niefunkcjonalne Platformy e-usług mieszkańca:</u>
1. Platforma musi być zaprojektowany w modelu trójwarstwowym:
- warstwa danych,
- warstwa aplikacji,
- warstwa prezentacji - przeglądarka internetowa - za pośrednictwem której następuje właściwa obsługa systemu przez użytkownika końcowego.
2. Platforma powinna umożliwiać pracę na bazie typu Open Source bądź na komercyjnym systemie bazodanowym.

3. Platforma w warstwie serwera aplikacji i bazy danych powinna mieć możliwość uruchomienia w środowiskach opartych na systemach operacyjnych z rodziny Windows lub równoważnych, oraz w środowiskach opartych na systemie Linux lub równoważnych.
4. Platforma w warstwie klienckiej powinna poprawnie działać w różnych środowiskach z minimum 5 najbardziej popularnymi przeglądarkami w Polsce w ich najnowszych wersjach (zgodnie ze statystyką prowadzoną na stronie http://gs.statcounter.com/ za okres 6 miesięcy poprzedzających miesiąc ogłoszenia postępowania określoną dla komputerów stacjonarnych „desktop").
5. Platforma powinna realizować wszystkie czynności przez przeglądarkę internetową.
6. Platforma musi pracować w wersji sieciowej z wykorzystaniem protokołu TCP/IP oraz być w pełni kompatybilny z sieciami TCP/IP.
7. Architektura Platformy powinna umożliwiać pracę jedno i wielostanowiskową, zapewniać jednokrotne wprowadzanie danych tak, aby były one dostępne dla wszystkich użytkowników.
8. W przypadku gdy Platforma do pracy wykorzystuje silnik bazy danych, baza taka musi być kompatybilna z systemem operacyjnym i musi istnieć możliwość jej instalacji i pracy na zasadach określonych dla Platformy.
9. Platforma w zakresie wydruków musi wykorzystywać funkcjonalność systemu operacyjnego i umożliwiać wydruk na dowolnej drukarce zainstalowanej i obsługiwanej w systemie operacyjnym, na którym zostanie zainstalowane oprogramowanie (drukarki lokalne, drukarki sieciowe).
10. Interfejs użytkownika (w tym administratora) powinien być w całości polskojęzyczny.
11. Dokumentacja powinna zawierać opis funkcji, wyjaśniać zasady pracy z programem oraz zawierać opisy przykładowych scenariuszy pracy.
12. Dokumentacja musi być dostępna z poziomu oprogramowania w postaci elektronicznej (pliki PDF, DOC lub RTF).
13. Platforma musi zapewniać weryfikację wprowadzanych danych w formularzach i kreatorach.
14. Platforma powinna zapewnić bezpieczeństwo danych zarówno na poziomie danych wrażliwych jak i komunikacji sieciowej przy zastosowaniu bezpiecznych protokołów sieciowych.
15. Platforma powinna być skalowalna, poprzez możliwość dołączenia dodatkowych stanowisk komputerowych, zwiększenie zasobów obsługujących warstwę aplikacyjną, zwiększenie zasobów obsługujących warstwę bazy danych.
16. Platforma powinna umożliwiać okresowe wykonywanie, w sposób automatyczny, pełnej kopii aplikacji i danych tego systemu.
17. Platforma powinna posiadać funkcjonalność zarządzania dostępem do tego systemu:
- administrator Platformy ma mieć możliwość tworzenia, modyfikacji oraz dezaktywacji kont użytkowników,
- administrator Platformy powinien móc nadawać uprawnienia użytkownikom,
- administrator Platformy powinien mieć możliwość przypisywać użytkowników do grup,
- powinna pozwalać na zmianę danych uwierzytelniających użytkownika (hasło).
18. Platforma powinna posiadać możliwość określenie maksymalnej liczby nieudanych prób logowania, po przekroczeniu której użytkownik zostaje zablokowany.
19. Platforma powinna się komunikować z systemami zewnętrznymi w sposób zapewniający poufność danych.
20. Platforma powinna być odporny na znane techniki ataku i włamań, typowe dla technologii, w której został wykonany.
21. Platforma powinna prowadzić dziennik zdarzeń (w postaci logów systemowych) i dostępu do obiektów danych, dokumentów, operacji na słownikach umożliwiający odtwarzanie historii aktywności poszczególnych użytkowników tego systemu oraz umożliwiać podgląd podstawowych statystyk użycia platformy.
22. Platforma musi działać w sposób responsywny – tzn. jej okno musi dostosować się do wyświetlacza urządzenia, z którego jest obsługiwana np. telefon, tablet.

<u>Wdrożenie Platformy eUsług Mieszkańca</u>
Wdrożenie ma na celu przeprowadzenie procesu umożliwiającego Zamawiającemu korzystanie z przedmiotu zamówienia.
1. Wykonawca ma obowiązek przeprowadzenia analizy przedwdrożeniowej obejmującej:
- analizę dotychczasowego sposobu organizacji pracy w obszarach e-usług,
- analizę bezpieczeństwa transmisji danych pomiędzy Systemami Dziedzinowymi,

- analizę możliwości integracji Platformy poprzez szynę danych z Systemami Dziedzinowymi oraz innymi Systemami.
2. Wykonawca ma obowiązek uzgodnienia z Zamawiającym Planu wdrożenia obejmującego:
- listę wymaganych czynności wykonywanych po stronie Zamawiającego,
- uzgodnienie sposobu odbioru procesu wdrożenia.
3. W ramach usług wdrożeniowych, Wykonawca:
- skonfiguruje warstwę sprzętową, systemową i sieciową gwarantując odpowiedni poziom bezpieczeństwa,
- uzgodni i wdroży poziom bezpieczeństwa w obszarze integracji,
- będzie dokonywał aktualizacji Platformy wraz z szyną danych na potrzeby realizacji projektu.
- dostarczy rozwiązania umożliwiające wymianę danych poprzez centralną szynę danych i uruchomi je na tej szynie,
- zapewni, że przepływ danych będzie się odbywać w formie szyfrowanej,
- umożliwi jednoczesną wymianę danych pomiędzy szyną i Platformą.

<u>Wdrożenie systemu obejmie również:</u>
1. instalację i konfigurację Platformy przy uzgodnieniu z Zamawiającym, wymaga się by to oprogramowanie było zainstalowane na infrastrukturze Zamawiającego.
2. Instruktaże oraz asystę stanowiskową dla administratora Platformy polegająca na:
- przeprowadzeniu instruktażu obsługi całego systemu bądź jego części wspomagającego obsługę obszarów działalności urzędu dla wskazanych przez urząd pracowników,
- przeprowadzeniu we współpracy z każdym wskazanym przez urząd pracownikiem analizy stanowiskowej zadań realizowanych w systemie charakterystycznych dla konkretnych merytorycznych stanowisk pracowniczych,
- przeprowadzeniu instruktażu w zakresie zarządzania użytkownikami i uprawnieniami, zabezpieczania i odtwarzania danych systemu dla osób pełniących obowiązki administratorów systemu wskazanych przez urząd.
3. Zapewnienie opieki powdrożeniowej Platformie w okresie trwania projektu (tj. na okres gwarancji i wsparcia podany w formularzu ofertowym, licząc od dnia podpisania końcowego protokołu odbioru dla tego zadania) polegającej na:
- świadczeniu pomocy technicznej,
- świadczeniu usług utrzymania i konserwacji dla dostarczonego oprogramowania,
- dostarczaniu nowych wersji oprogramowania będących wynikiem wprowadzenia koniecznych zmian w funkcjonowaniu systemu związanych z wejściem w życie nowych przepisów,
- dostosowaniu do obowiązujących przepisów nie później niż w dniu ich wejścia w życie, chyba że, zmiany prawne nie zostały ogłoszone z minimum 30-dniowym terminem poprzedzającym ich wprowadzenie w życie. W przypadku, jeżeli zmiany nie zostały ogłoszone z minimum 30-dniowym terminem poprzedzającym ich wprowadzenie w życie Wykonawca zobligowany jest do ich wprowadzenia w ciągu 30 dni roboczych od dnia wprowadzenia przepisu w życie,
- dostarczaniu nowych, ulepszonych wersji oprogramowania lub innych komponentów systemu będących konsekwencją wykonywania w nich zmian wynikłych ze stwierdzonych niedoskonałości technicznych,
- dostarczaniu nowych wersji dokumentacji użytkownika oraz dokumentacji technicznej zgodnych co do wersji jak i również zakresu zaimplementowanych i działających funkcji z wersją dostarczonego oprogramowania aplikacyjnego,
- świadczeniu telefonicznie usług doradztwa i opieki w zakresie eksploatacji systemu.
- podejmowaniu czynności związanych z diagnozowaniem problemów oraz usuwaniem przyczyn nieprawidłowego funkcjonowania dostarczonego rozwiązania.

<u>Wymaga się udzielenia gwarancji i wsparcie na platformę eUsług na okres min 12 miesięcy</u>
Po wdrożeniu Wykonawca przekaże Zamawiającemu wszelkie niezbędne dokumenty w celu umożliwienia mu korzystania z Platformy. Dokumenty jakie powinny zostać przekazane to:
Pełna dokumentacja powykonawcza obejmująca:
- opis techniczny procedur aktualizacyjnych,

- dostarczenie wszelkich niezbędnych materiałów uzupełniających do powyższej dokumentacji powykonawczej, które są konieczne do właściwej eksploatacji systemu,
- instrukcje użytkownika i administratora wdrożonego systemu.

Przygotowanie i przeprowadzenie pakietów szkoleń z Platformy eUsług Mieszkańca

Szkolenia mają na celu osiągniecie odpowiedniej wiedzy z zakresu używania systemu na odpowiednich stanowiskach służbowych. Przeprowadzenie pakietu szkoleń powinno zostać odpowiednio skoordynowane z przeprowadzeniem procesu wdrożenia.

1. Szczegółowy zakres poszczególnych szkoleń będzie podlegał uzgodnieniu pomiędzy Wykonawcą a Zamawiającym w ramach akceptacji harmonogramu i materiałów szkoleniowych oraz analizy przedwdrożeniowej.
2. Wykonawca na etapie uzgadniania materiałów szkoleniowych przekaże minimalne wymagania, jakie powinni spełniać oddelegowani przez Zamawiającego, uczestnicy szkolenia.
3. Do każdego modułu wspomagającego obsługę obszarów działalności urzędu, Zamawiający wskaże osoby, które Wykonawca przeszkoli.
4. Szkolenia będą realizowane w pomieszczeniach i na sprzęcie udostępnionym przez Urząd.
5. Zamawiający nie dopuszcza przeprowadzania szkoleń typu e-learning w zastępstwie szkoleń tradycyjnych, jednak dopuszcza szkolenia zdalne (sesje zdalnego pulpitu, webinaria).
6. Zamawiający dopuszcza przeprowadzanie szkoleń grupowych, w grupach do 10 użytkowników oraz szkoleń indywidualnych przy stanowiskowych dla grup jedno-, dwu- lub trzyosobowych.
7. Wykonawca przeszkoli osoby pełniące obowiązki administratorów wskazanych przez Zamawiającego w zakresie zarządzania użytkownikami i uprawnieniami, zabezpieczania i odtwarzania danych.
8. Wykonawca zapewni przeszkolenie administratora wskazanego przez Zamawiającego w zakresie administracji i konfiguracji zaoferowanego systemu bazodanowego. Szkolenie musi obejmować co najmniej instalację, konfigurację bazy danych, obsługę narzędzi administratora, architekturę systemu, zagadnienia związane z zachowaniem bezpieczeństwa, integralności i zabezpieczenia przed utratą danych, przywracaniem danych po awarii.
9. Uzgodnieniu pomiędzy stronami podlegają:
- minimalne wymagania dla uczestników szkoleń,
- harmonogram szkoleń grupowych i indywidualnych,
- materiały szkoleniowe dla szkoleń grupowych,
- listy obecności ze szkoleń grupowych i indywidualnych.

Zamawiający oczekuje, że ilość oraz program szkoleń powinny gwarantować użytkownikom systemu zapoznanie się z wszystkimi funkcjonalnościami jakie system oferuje i pozwalać pracownikom na rozpoczęcie pracy w systemie.

Integracja Platformy eUsług Mieszkańca z Systemem Dziedzinowym (Zintegrowany System Respons)

W celu dostarczenia zaawansowanych usług elektronicznych dla mieszkańców i przedsiębiorców konieczne jest również dostarczenie usług integracji SD (Systemów Dziedzinowych) na potrzeby Platformy.
Integracja ta ma na celu udostępnienie aktualnych informacji finansowych (należności, płatności) z poziomu Systemów Dziedzinowych. Integracja będzie możliwa do realizacji, o ile Systemy Dziedzinowe i pozostałe Systemy Zamawiającego (np. systemy odczytu i rozliczeń za wodę) będą posiadały dostarczone interfejsy integracyjne w opisanym zakresie.

Poniższa lista opisuje minimalny zakres integracji Platformy z Systemami Dziedzinowymi. Integracja od strony Systemów Dziedzinowych i pozostałych Systemów (np. systemy odczytu i rozliczeń za wodę) musi się odbywać poprzez Szynę Danych.

1. SD zintegrowany z Platformą, powinien udostępniać informację o kontrahentach w zakresie nie mniejszym niż: Nazwa/Nazwisko, Imię, PESEL, NIP, adres z uwzględnieniem wskazań na słownik TERYT.
2. SD integrowany z Platformą powinien udostępniać informacje o należnościach kontrahenta (mieszkańca).

3. Informacje dot. należności nie mogą mieć mniejszego zakresu niż: rodzaj należności, kwota, kwota do zapłaty, kwota odsetek, VAT, numer decyzji urzędowej, termin płatności.
4. SD integrowany z Platformą powinien udostępniać informacje dotyczące kont bankowych, na które należy wpłacić należność. Systemy Dziedzinowe i pozostałe Systemy muszą uwzględnić te nr rachunków w celu przyjmowania masowych płatności.
5. SD integrowany z Platformą powinien udostępniać informacje dotyczące wpłat dokonanych na należności. Przekazane dane muszą zawierać zakres informacyjny przynajmniej: data wpłaty, kwota, kwota odsetek, kwota VAT, kontrahent (mieszkaniec) wpłacający.
6. SD integrowany z Platformą powinien udostępniać szczegółowe informacje dla należności do zapłaty będących wezwaniami lub upomnieniami takie jak: data odbioru, data wydania, data zapłaty, koszt, numer.
7. SD lub inny System Zamawiającego integrowany z Platformą musi umożliwiać podanie należności z określeniem: nazwy, typu, kwoty, terminu płatności, kontrahenta.
Zamawiający uwzględnia, że poszczególne Systemy Dziedzinowe lub pozostałe Systemy Zamawiającego (np. systemy odczytu i rozliczeń za wodę) mogą nie dysponować zakresem danych do udostępnienia zgodnym z powyższą tabelą. Przykładowo System Dziedzinowy nie prowadzi należności z tytułu zezwolenia na sprzedaż alkoholu. Wykonawca nie ma wtedy obowiązku wykazać, że integracja tego typu danych się odbyła. Zakres integracji musi być poprzedzony analizą przedwdrożeniową, i powinien być przekazany Zamawiającemu do akceptacji.
Wykonawca, który dostarczy Platformę e-Usług Mieszkańca, jest zobowiązany na żądanie Zamawiającego udostępnić je poszczególnym autorom Systemów Dziedzinowych lub Systemów w celu umożliwienia integracji z Platformą.

Wymagania sprzętowe:
<u>Wykonawca zapewnia odpowiednie serwery i urządzenia na potrzeby Platformy e-Usług oraz hosting na okres min. 12 miesięcy</u>
Wymagania do hostingu:
System wraz z Szyną Danych zostanie zainstalowany w siedzibie wykonawcy na terenie Polski.
Bezpieczeństwo zostanie zapewnione poprzez zastosowanie następujących redundantnych elementów:
• Wydajne macierze dyskowe, serwery oraz urządzenia światłowodowe
• Bezpieczeństwo zasilania zagwarantowane dwoma niezależnymi obwodami z automatycznym bypassem oraz systemem awaryjnym UPS i generatorem prądu który podtrzyma infrastrukturę przez okres nieograniczony
• Gwarancja niezawodności dostępu przez sieć Internet, tj. wyposażenie w minimum dwa niezależne łącza z routingiem
• Redundantne klimatyzatory pozwalające utrzymać odpowiednie warunki temperatury oraz wilgotności
Dane z macierzy dyskowych będę zabezpieczane na dedykowanym serwerze backupowym.
Sprzęt, na którym będzie hostowany system będzie posiadał zagwarantowane bezpieczeństwo przeciwpożarowe tj. pomieszczenia wyposażone w niepalną podłogę techniczną oraz system kontroli przeciwpożarowej.
Sprzęt, na którym będzie hostowany system będzie posiadał zagwarantowane bezpieczeństwo fizyczne tj. dostęp do pomieszczeń i sprzętu będzie ograniczony dla upoważnionych pracowników wyposażonych w elektroniczną kontrolę dostępu, monitoring pomieszczeń w systemie 24/7/365, system antywłamaniowy oraz ochrona przez licencjonowaną firmę ochroniarską.
Wykonawca świadczy usługę hostingu w zagwarantowanie SLA 99% oraz z szybkością połączenia nie mniej niż 5Mb/s
Wykonawca będzie świadczył usługę Administrowania serwerami przeznaczonymi dla Systemu
Wykonawca będzie świadczył usługę monitoringu systemu i aplikacji poprzez dedykowany serwer monitoringu i logów.
Wykonawca musi posiadać wdrożony system Zarzadzania Bezpieczeństwem Informacji
Do czasu SLA nie wliczane są okna serwisowe uzgodnione z Zamawiającym.

<u>Formularze elektroniczne</u>
Tworzenie formularzy elektronicznych – ogólne wymagania.

a. Formularze elektroniczne powinny być tworzone z wykorzystaniem języka XForms oraz XPath.
b. Wykonawca opracuje formularze elektroniczne (zgodnie z właściwymi przepisami prawa) na podstawie przekazanych przez Zamawiającego kart usług z formularzami w formacie edytowalnym.
c. Wszystkie formularze elektroniczne Wykonawca przygotuje z należytą starannością tak, aby pola do uzupełnienia w tych formularzach zgadzały się z polami formularzy w formacie edytowalnym.
d. Pola wskazane przez Zamawiającego jako pola obowiązkowe w formularzach w formacie edytowalnym, muszą zostać polami obowiązkowymi również w formularzach elektronicznych.
e. Układ graficzny wszystkich formularzy powinien być w miarę możliwości jednolity.
f. Wizualizacja formularzy elektronicznych nie musi być identyczna ze wzorem w formacie edytowalnym, ale musi zawierać dane w układzie niepozostawiającym wątpliwości co do treści i kontekstu zapisanych informacji, w sposób zgodny ze wzorem.
g. Przygotowując formularze Wykonawca musi dążyć do maksymalnego wykorzystania słowników.
h. W budowanych formularzach należy wykorzystać mechanizm automatycznego pobierania danych z profilu zaufanego – celem uzupełnienia danych o wnioskodawcy.
i. Formularze muszą zapewniać walidację wprowadzonych danych po stronie klienta i serwera zgodnie z walidacją zawartą w schemacie dokumentu.
j. Jeśli w formularzu elektronicznym występują pola PESEL, REGON lub kod pocztowy, to pola te muszą być walidowane pod kątem poprawności danych wprowadzanych przez wnioskodawcę.
k. Każdy opracowany przez Wykonawcę formularz (w postaci pliku XML) musi zostać przekazany Zamawiającemu na okres 7 dni roboczych w celu dokonania sprawdzenia i wykonania testów na formularzu.
l. Po okresie testów, o których mowa w wymaganiu poprzednim, Zamawiający przekaże Wykonawcy ewentualne poprawki i uwagi dotyczące poszczególnych formularzy, które Wykonawca usunie w ciągu 7 dni.
m. Wykonawca przygotuje wzory dokumentów elektronicznych zgodnie ze standardem ePUAP w formacie XML zgodnym z formatem Centralnego Repozytorium Wzorów Dokumentów.
n. Zamawiający dopuszcza możliwość wykorzystania przez Wykonawcę wzorów, które są już opublikowane w CRWD po akceptacji Zamawiającego.
o. Wygenerowane dla poszczególnych formularzy wzory dokumentów elektronicznych, składające się z plików:
i. wyróżnik (wyroznik.xml),
ii. schemat (schemat.xml),
iii. wizualizacja (styl.xsl),
muszą zostać dostosowane do wymogów formatu dokumentów publikowanych w CRWD i spełniać założenia interoperacyjności.
p. W ramach projektu Wykonawca przygotuje i przekaże Zamawiającemu wszystkie wzory dokumentów elektronicznych w celu złożenia wniosków o ich publikację w CRWD (jeżeli będzie taka konieczność).
W przypadku, jeżeli system teleinformatyczny ePUAP będzie dawał możliwość publikacji formularzy elektronicznych na etapie realizacji zamówienia przewiduje się dodatkowo wykonanie następujących prac:
a. Bazując na przygotowanych wzorach dokumentów elektronicznych oraz opracowanych na platformie ePUAP formularzach elektronicznych Wykonawca przygotuje instalacje aplikacji w środowisku ePUAP.
b. Aplikacje muszą być zgodne z architekturą biznesową ePUAP oraz architekturą systemu informatycznego ePUAP.
c. Przygotowane aplikacje muszą zostać zainstalowane przez Wykonawcę na koncie ePUAP Zamawiającego.
d. Zainstalowane aplikacje muszą spełniać wymogi ePUAP oraz pozytywnie przechodzić przeprowadzone na ePUAP walidacje zgodności ze wzorami dokumentów.
e. Na czas realizacji projektu Zamawiający zapewni Wykonawcy dostęp do części administracyjnej platformy ePUAP konta JST z uprawnieniami do konsoli administracyjnej Draco, ŚBA i usług.
f. W przypadku zwłoki w publikacji wzorów dokumentów CRWD realizowanej przez Ministerstwo Cyfryzacji (administrator ePUAP) dopuszcza się dokonanie odbioru tej części zamówienia w ramach lokalnej publikacji w CRWD z zastrzeżeniem, że Wykonawca dokona przekonfigurowania aplikacji po pomyślnej publikacji CRWD przez Ministerstwo Cyfryzacji.
g. Zamawiający przekaże Wykonawcy opisy usług w formacie edytowalnym.
h. Zamawiający dopuszcza, aby Wykonawca wykorzystał opis usług, które są umieszczone na platformie ePUAP po akceptacji opisu usługi przez Zamawiającego.

i. Zadaniem Wykonawcy jest odpowiednie powiązanie opisów usług zamieszczonych na ePUAP z odpowiednimi usługami.
j. Wykonawca przygotuje definicję brakujących opisów usług na ePUAP oraz udzieli wsparcia Zamawiającemu, który zwróci się do Ministerstwa Cyfryzacji w celu akceptacji i umieszczenia ich na platformie ePUAP.
k. Wszystkie opisy usług zostaną przyporządkowane do jednego lub więcej zdarzenia życiowego z Klasyfikacji Zdarzeń, a także do Klasyfikacji Przedmiotowej Usług ePUAP.
l. W przypadku, jeżeli system teleinformatyczny ePUAP nie będzie dawał możliwości publikacji formularzy elektronicznych na etapie realizacji zamówienia, przewiduje się przygotowanie i przeprowadzenie procesu instalacji formularzy elektronicznych przez Wykonawcę na określonej do pełnienia tej funkcji ogólnopolskiej platformie.

b) Moduł do systemu dziedzinowego Urzędu Miejskiego w Sędziszowie – 1 szt.

Moduł musi zapewniać możliwość przypisania indywidualnego numeru rachunku do kartoteki skojarzonej z rodzajem należności:
- konfigurację i generowanie kont indywidualnych i identyfikatorów dla tytułów przelewów,
- importy plików XML z banków spółdzielczych,
- rozliczenia przelewów bankowych z windykacją włącznie,
- obsługę wydruku informacji o indywidualnym numerze rachunku lub identyfikatorze do umieszczenia w tytule przelewu dla decyzji w module GODP,
- wydruki przelewu wpłat (załączane do decyzji),
- wydruki informacji o indywidualnym numerze rachunku lub identyfikatorze do umieszczenia w tytule przelewu na dokumentach z informacjami dla płatników dla decyzji w modułach Podatki od osób fizycznych (Grunty), Podatki od osób prawnych(OP)), Podatki od środków transportu, koncesje alkoholowe, Nieruchomości, Faktury, Psy,
- integracja z platformą ePłatności dla mieszkańców,
- wydruk kodów kreskowych na poleceniu przelewu,
- rozpoznanie przelewów masowych pod kątem integracji z modułem FK i wparcia dla użytkowników w dekretowaniu przelewów przychodzących.

Indywidualny numer rachunku musi zapewnić możliwość rozpoznania na rzecz, jakiego podmiotu została wykonana wpłata oraz z jakiego tytułu tą wpłatę wykonano. Dla płatności wykonywanych za pośrednictwem serwisu www ePłatności możliwe będzie również ustalenie, na podstawie danych przekazanych w tytule przelewu, konkretnej należności, jaka została uregulowana. Użytkownik końcowy (klient) JST, adresat np. Decyzji związanej z ustaleniem wysokości podatku)
- ma możliwość uregulowania opłaty za pośrednictwem portalu e-Płatności;
- ma wgląd w informacje o własnych zobowiązaniach (e-Płatności);
- otrzyma na dokumencie określającym wysokość zobowiązania indywidualny numer rachunku, na który ma regulować własne zobowiązania

Nr referencyjny: IN.271.1.2022

8. Zakup oprogramowania

Program - Zarządzanie uprawnieniami i licencjami - 1 szt.

Lista funkcjonalności:

1. Funkcjonalności ogólne

System odpowiedzialny za zarządzanie licencjami, monitorowanie ich terminu ważności, zarządzanie uprawnieniami z dowolnych systemów w ramach pracy jednostki organizacyjnej, procesem akceptacji przydzielanych uprawnień, integracji w zakresie możliwości nadawania uprawnień w systemach zintegrowanych, użytkownikami i uprawnieniami w aplikacji do zarządzania licencjami i uprawnieniami, zarządzaniem parametrami, zadaniami wsadowymi, monitoringiem wykonanych czynności oraz sterowanie wysyłką powiadomień za pośrednictwem brokera powiadomień, który zapewnia mechanizm wysyłki powiadomień dowolnym kanałem komunikacji (SMS, eMail, poprzez dedykowane interfejsy).

1. System umożliwia definiowanie dowolnej ilości użytkowników.
2. System w całości spolonizowany, a więc posiada polskie znaki i instrukcję obsługi po polsku dla użytkownika oraz administratora.
3. System posiada graficzny interfejs użytkownika gwarantujący wygodne wprowadzanie danych, przejrzystość prezentowania danych na ekranie oraz wygodny sposób wyszukiwania danych po ergonomicznie dobranych kryteriach.
4. System gwarantuje integralność danych, bieżącą kontrolę poprawności wprowadzanych danych, spójność danych.
5. System pracuje w środowisku sieciowym i posiada wielodostępność pozwalającą na równoczesne korzystanie z bazy danych przez wielu użytkowników.
6. System gwarantuje możliwość wdrożenia integracji z Systemami Dziedzinowymi oraz innymi Systemami. Za integrację odpowiada szyna danych WSO2 ESB.
7. System posiada mechanizmy umożliwiające weryfikację integralności danych tj. identyfikację użytkownika i ustalenie daty wprowadzenia i modyfikacji danych. W systemie jest dostępny dziennik zdarzeń systemowych zapewniający pełną rozliczalność przez przechowywanie szczegółów dotyczących wykonywania każdej czynności wykonanej przez wszystkich użytkowników.
8. System posiada mechanizmy ochrony danych przed niepowołanym dostępem, nadawania uprawnień dla użytkowników do korzystania z modułów jak również do korzystania z wybranych funkcji. System jest oparty o mechanizm ról i uprawnień.

2. Lista funkcjonalności Systemu do zarządzania uprawnieniami i licencjami

1. System umożliwia bezpieczne zalogowanie poprzez przeglądarkę.
2. System, oprócz logowania standardowego (eMail i hasło) umożliwia logowanie domenowe.
3. Użytkownik ma możliwość zmiany hasła oraz ponownego jego nadania w przypadku zagubienia hasła.
4. System udostępnia użytkownikowi o charakterze administratora funkcjonalności zarządzania konfiguracją systemu, w tym przegląd i modyfikację bieżących ustawień systemu, które wpływają na jego zachowanie.
5. System pozwala administratorowi na zarządzanie konfiguracją zadań wsadowych, czyli zadań, które uruchamiane są w cyklicznie zdefiniowanych momentach (dniach, godzinach, minutach, itp.).
6. System posiada funkcje umożliwiające zapis, odczyt i usunięcie plików w systemie.
7. System umożliwia przegląd rejestru licencji dodanych w aplikacji, z możliwością filtrowania po następujących kryteriach:
a. Nazwa licencji;
b. Rodzaj licencji;

c. Data obowiązywania od;
d. Data obowiązywania do;
e. Status;
f. Przypisany użytkownik.
8. System pozwala na sortowanie rosnąco i malejąco wyświetlanych danych rejestru licencji po wartościach: rodzaj, nazwa, data obowiązywania od, do, status.
9. System udostępnia możliwość wydruku raportu licencji.
10. System posiada funkcje umożliwiające podgląd danych szczegółowych licencji przez uprawnionego użytkownika aplikacji, w tym przegląd danych podstawowych, dołączonych dokumentów oraz przypisanych użytkowników.
11. System udostępnia funkcjonalność monitorowania i powiadamiania (eMail) o kończącym się terminie ważności danej licencji.
12. System udostępnia możliwość przypisania (odebrania) dowolnej licencji wskazanemu pracownikowi wraz z możliwością wysłania maila o tym fakcie z danymi dostępowymi w przypadku przypisania licencji.
13. System umożliwia definiowanie dowolnych uprawnień. Dla tworzonych uprawnień istnieje możliwość określenia atrybutów m.in.: nazwa, notatka, szablon opisu uprawnienia (domyślna treść wysyłana przy nadawaniu).
14. System dla zdefiniowanego uprawnienia udostępnia możliwość ustawienia wysyłki powiadomienia (eMail) przy nadawaniu / odbieraniu uprawnienia.
15. System umożliwia tworzenie dowolnych grup uprawnień, co pozwala na definiowanie zbiorów uprawnień niezbędnych do przypisania np. na danym stanowisku, bez konieczności przypisywania pojedynczych uprawnień.
16. System umożliwia przypisanie administratorów do uprawnień, którzy będą odpowiedzialni za fizyczne nadanie / odebranie oraz potwierdzenie uprawnienia.
17. System udostępnia funkcjonalność określania ścieżki akceptacyjnej dla danego uprawnienia. Definiując dane uprawnienia istnieje możliwość określenia konkretnej listy stanowisk / pracowników, którzy będą potwierdzać nadanie / odebranie uprawnienia. Opcjonalnie można ustawić dla uprawnienia akceptację automatyczną.
18. System posiada funkcjonalność powiadamiania eMail o zatwierdzeniu / odrzuceniu akceptacji na poszczególnych poziomach ścieżki akceptacyjnej.
19. System posiada rejestr zgłoszonych uprawnień do akceptacji, z możliwością przeglądu danych historycznych.
20. System udostępnia funkcjonalność tworzenia dowolnych ścieżek akceptacyjnych, prowadzenia rejestru zdefiniowanych ścieżek wraz z ich zarządzaniem.
21. System posiada funkcjonalność rejestru nadanych uprawnień z możliwością wyszukiwania min. według pracowników, uprawnieniach oraz data obowiązywania, nadania. W rejestrze można zgłosić potrzebę nadania / odebrania danego uprawnienia pracownikowi. Zgłoszenie dostępne będzie w kontekście pojedynczego uprawnienia, wybranych uprawnień, jak również uprzednio zdefiniowanej grupy uprawnień.

3. Ograniczenia niefunkcjonalne spełniane przez System do zarządzania uprawnieniami i licencjami
1. System jest zaprojektowany w modelu trójwarstwowym:
- warstwa danych,
- warstwa aplikacji,
- warstwa prezentacji - przeglądarka internetowa - za pośrednictwem której następuje właściwa obsługa systemu przez użytkownika końcowego.
2. System umożliwia pracę na bazie typu Open Source, bądź na komercyjnym systemie bazodanowym.
3. W warstwie serwera aplikacji i bazy danych istnieje możliwość uruchomienia systemu w środowiskach opartych na systemach operacyjnych z rodziny Windows lub równoważnych oraz w środowiskach opartych na systemie Linux lub równoważnych.
4. System w warstwie klienckiej działa w różnych środowiskach z minimum 5 najbardziej popularnymi przeglądarkami w Polsce w ich najnowszych wersjach (zgodnie ze statystyką prowadzoną na stronie

http://gs.statcounter.com/ za okres 6 miesięcy poprzedzających miesiąc ogłoszenia postępowania określoną dla komputerów stacjonarnych „desktop").
5. System realizuje wszystkie czynności przez przeglądarkę internetową.
6. System pracuje w wersji sieciowej z wykorzystaniem protokołu TCP/IP oraz jest w pełni kompatybilna z sieciami TCP/IP.
7. Architektura systemu umożliwia pracę jedno i wielostanowiskową, zapewnia jednokrotne wprowadzanie danych tak, aby były one dostępne dla wszystkich użytkowników.
8. W przypadku gdy system do pracy wykorzystuje silnik bazy danych, baza jest kompatybilna z systemem operacyjnym i istnieje możliwość jej instalacji i pracy na zasadach określonych dla systemu.
9. System w zakresie wydruków wykorzystuje funkcjonalność systemu operacyjnego i umożliwia wydruk na dowolnej drukarce zainstalowanej i obsługiwanej w systemie operacyjnym, na którym zostanie zainstalowane oprogramowanie (drukarki lokalne, drukarki sieciowe).
10. Interfejs użytkownika (w tym administratora) jest w całości polskojęzyczny.
11. System zapewnia weryfikację wprowadzanych danych w formularzach i kreatorach.
12. System zapewnia bezpieczeństwo danych zarówno na poziomie danych wrażliwych jak i komunikacji sieciowej przy zastosowaniu bezpiecznych protokołów sieciowych.
13. System umożliwia okresowe wykonywanie, w sposób automatyczny, pełnej kopii aplikacji i danych systemu.
14. System posiada funkcjonalność zarządzania dostępem do aplikacji:
- administrator systemu ma możliwość tworzenia, modyfikacji oraz dezaktywacji kont użytkowników,
- administrator systemu może nadawać uprawnienia użytkownikom,
- pozwala na zmianę danych uwierzytelniających użytkownika (hasło).
15. System posiada możliwość określenia maksymalnej liczby nieudanych prób logowania, po przekroczeniu której użytkownik zostaje zablokowany.
16. System komunikuje z systemami zewnętrznymi w sposób zapewniający poufność danych.
17. System jest odporny na znane techniki ataku i włamań, typowe dla technologii, w której został wykonana.
18. System prowadzi dziennik zdarzeń (w postaci logów systemowych) i umożliwia dostęp do obiektów danych, dokumentów, operacji na słownikach umożliwiający odtwarzanie historii aktywności poszczególnych użytkowników systemu oraz umożliwia podgląd podstawowych statystyk użycia systemu.

4. Integracja systemu zarządzania uprawnieniami i licencjami z systemami dziedzinowymi i zewnętrznymi
1. Zakres integracji dotyczy przede wszystkim:
a. Z systemem dziedzinowym (integracja zgodnie z pkt. 6) w zakresie powiadamiania (eMail) wybranych przełożonych / stanowisk o konieczności nadania odpowiednich uprawnień przy zatrudnianiu danego pracownika. Analogiczna opcja dostępna w przypadku zakończenia trwania umowy.
b. Z dowolnym (integracja zgodnie z pkt. 6) systemem posiadającym prostą siatkę uprawnień / ról w zakresie nadawania / odbierania poszczególnych uprawnień pracownikom danej jednostki organizacyjnej.
c. Z dowolnym (integracja zgodnie z pkt. 6) systemem posiadającym rozbudowaną siatkę uprawnień / ról w zakresie odebrania wszystkich uprawnień pracownikom JST.
d. Z dowolnym (integracja zgodnie z pkt. 6) systemem w zakresie aktywowania / zawieszania konta wybranego pracownika danej jednostki organizacyjnej.

5. Funkcjonalności dot. Szyny Danych (ESB)
1. Komunikacja pomiędzy Systemem i zintegrowanymi systemami dziedzinowymi, jak również pomiędzy systemami zewnętrznymi jest realizowana przez pośrednią warstwę integracyjną Szynę Danych.
2. ESB odpowiada za:
- rejestrację usług sieciowych oferowanych przez Systemy Dziedzinowe oraz System w ramach dowolnej sieci opartej o protokół TCP/IP
- rejestrowanie potwierdzeń i statusów przekazania i przyjęcia informacji przez komunikujące się systemy: obsługę sytuacji polegających na chwilowej utracie łączności z warstwą integracyjną przez jeden lub kilka komunikujących się systemów.
3. ESB umożliwia prezentację w graficznym interfejsie użytkownika informacji w zakresie monitorowania wymiany danych oraz diagnozowania problemów z przekazywaniem danych.

4. ESB posiada wbudowane narzędzie do tworzenia, implementowania, wdrażania, uruchamiania i konfigurowania usług wymiany danych pomiędzy systemami zewnętrznymi.
5. ESB umożliwia podłączanie, katalogowanie i wzajemne udostępniania usług pomiędzy systemami integrowanymi: System do zarządzania uprawnieniami i licencjami, systemy dziedzinowe i systemy zewnętrzne.
6. ESB umożliwia obsługę protokołu SOAP dla usług wywoływanych oraz usług udostępnianych. Musi zapewniać:
- realizację wywoływania lub udostępniania w standardzie min. WSDL, SOAP,
- standard WS-Security.
7. ESB umożliwia realizację procesów integracyjnych w oparciu o model synchroniczny i asynchroniczny.

9. Szkolenia pracowników z cyberbezpieczeństwa

Minimalny okres świadczenia usług minimum 3 lata. Kapitał zakładowy wynoszący minimum 76.000.000,00 zł. Firma realizująca audyt powinna mieć zatrudnionych specjalistów zakresów: SECURITY AWARENESS (dział szkoleń).

Rekomendacje dotyczące szkoleń z certyfikatami w ilości 3 sztuk.

Udostępnienie szkolenia w postaci filmów instruktażowych z możliwością ich dalszego udostępniania pracownikom w instytucji Zamawiającego.

Dożywotnia licencja na wykorzystanie filmów szkoleniowych przez Zamawiającego

Udostępnione materiały szkoleniowe zakończone testem pozwalającym uzyskać certyfikat ukończenia szkolenia.

Tematyka szkoleń:

1. Zagrożenia w cyberprzestrzeni,
2. Socjotechnika, mechanika ataku z wykorzystaniem socjotechniki,
3. Inżynieria społeczna na przykładzie reguł Cialdiniego, wykorzystanie ludzkich słabości,
4. Przykłady phishingu – Poczta Polska, sklepy internetowe, OLX, InPost, banki, instytucje, wykorzystanie stanu wyjątkowego (pandemia Covid-19),
5. Wskazówki – co zrobić, by uniknąć ataku.
6. Bezpieczne korzystanie z mediów społecznościowych,
7. Gdzie czai się zagrożenie – wykorzystanie mediów społecznościowych podczas ataku spearphishingowego,
8. Dane, jakie zbiera o nas Facebook,
9. Przejęcie konta, kradzież tożsamości – zagrożenie zarówno dla firm jak i końcowego użytkownika,
10. Jak ustrzec się ataku w mediach społecznościowych,
11. Fakenews – charakterystyka, konsekwencje, jak się przed nimi bronić.
12. Zagrożenia w obszarze bankowości, skimming, phishing bankowy, vishing, jak ich uniknąć,
13. Ataki typu man in the middle, man in the browser, charakterystyka i mechanika ataku,
14. Złośliwe oprogramowanie w telefonie, trojany bankowe – jak dbać o bezpieczeństwo smartfonów,
15. Bankowość, trojany i hasła – kontynuacja poprzedniego odcinka,
16. Oznaki zainfekowania złośliwym oprogramowaniem,
17. Hasła – silne hasło, wskazówki, metoda budowy bezpiecznego hasła, manager haseł, biometria,
18. Jak sprawdzić, czy nasze dane wyciekły?

19. Co zrobić w przypadku wycieku danych?
20. Atak z wykorzystaniem spearphishingu – przykład ataku, mechanika, zbieranie informacji (tzw. biały wywiad)
21. Atak typu DDoS – mechanika ataku, przykłady
22. Atak typu ransomware, mechanika, zagrożenia
23. Ataki WannaCry i Petya – skutki
24. Co zrobić w przypadku infekcji złośliwym oprogramowaniem? Jak się zabezpieczyć
25. Bezpieczeństwo pracy zdalnej

10. Zakup zabezpieczeń logicznych (zapory UTM)

a) Zapory UTM – 3 szt.

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

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

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 5 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.

4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są 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. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje 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.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje 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.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - 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.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia 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 posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.

9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

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

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania). Konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej – opisanej w sekcji Centralny system logowania.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.

4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Certyfikaty

Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

b) System analizy UTM – 1 szt.

Wymagania Ogólne

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Interfejsy, Dysk:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB.

Nr referencyjny: IN.271.1.2022

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:

a. Listę najczęściej wykrywanych ataków.
b. Listę najbardziej aktywnych użytkowników.
c. Listę najczęściej wykorzystywanych aplikacji.
d. Listę najczęściej odwiedzanych stron www.
e. Listę krajów , do których nawiązywane są połączenia.
f. Listę najczęściej wykorzystywanych polityk Firewall.
g. Informacje o realizowanych połączeniach IPSec.

4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
   - Malware.

- Aplikacje sieciowe.
- Email.
- IPS.
- Traffic.
- Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy i licencje

1. System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
2. Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Nr referencyjny: IN.271.1.2022

Dla części nr II

1. Laptopy – 46 szt.

Nazwa	Wymagane minimalne parametry techniczne
Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, dostępu do Internetu oraz poczty elektronicznej,
Matryca	Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości FHD (1920 x 1080) z podświetleniem LED matryca matowa, jasność min. 220 nits, kontrast 400:1
Wydajność	Notebook w oferowanej konfiguracji musi osiągać w teście Bapco Sysmark25 wyniki nie gorsze niż: Productivity – minimum 1025 punktów Creativity – minimum 880 pkt Responsiveness – minimum 786 pkt Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.) Potwierdzeniem spełnienia powyższych wymagań będzie dołączony do oferty wydruk raportu z oprogramowania testującego. Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych testów Wykonawca może zostać wezwany przy dostawie do wykonania w obecności Zamawiającego, na dwóch losowo wskazanych przez Zamawiającego notebookach, testów ich wydajności, zgodnie z powyższymi wymaganiami, potwierdzający zadeklarowane przez Wykonawcę wyniki wydajnościowe
Pamięć RAM	8GB DDR4 możliwość rozbudowy do min 16GB, dwa sloty pamięci (nie dopuszcza się pamięci wlutowanych); możliwość rozbudowy pamięci przez użytkownika, bez kontaktu z serwisem producenta.
Pamięć masowa	min. 256 GB SSD NVMe, fabryczna możliwość instalacji drugiego dysku 2,5”
Karta graficzna	Zintegrowana z procesorem
Multimedia	Dwukanałowa karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki stereo o średniej mocy min. 2x 2W, cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy. Kamera internetowa o rozdzielczości min. HD trwale zainstalowana w obudowie matrycy, dioda informująca użytkownika o aktywnej kamerze.
Bateria i zasilanie	Czas pracy na baterii minimum 390 minut potwierdzony przeprowadzonym testem MobileMark 2018 Battery Life (do oferty załączyć wydruk przeprowadzonego testu) Zasilacz o mocy min. 65W. Konstrukcja komputera musi umożliwiać demontaż samej baterii lub wszystkich zainstalowanych baterii, samodzielnie bez udziału serwisu w okresie gwarancyjnym.

	Bateria nie może być trwale zespolona z płytą główną.
Waga	Waga komputera z oferowaną baterią nie większa niż 1,7 kg
Obudowa	Obudowa notebooka wzmocniona, szkielet i zawiasy notebooka wykonany z wzmacnianego metalu.
BIOS	BIOS zgodny ze specyfikacją UEFI, pełna obsługa za pomocą klawiatury i myszy. BIOS musi umożliwiać przeprowadzenia inwentaryzacji sprzętowej poprzez wyświetlenie informacji o: wersji BIOS, numerze seryjnym i dacie produkcji komputera, wielkości, prędkości i sposobie obsadzenia zainstalowanej pamięci RAM, typie zainstalowanego procesora, zainstalowanym dysku twardym (pojemność, model), MAC adresie wbudowanej w płytę główną karty sieciowej. Funkcja blokowania/odblokowania portów USB Możliwość, ustawienia hasła dla administratora oraz użytkownika dla BIOS'u, po podaniu hasła użytkownika możliwość jedynie odczytania informacji, brak możliwości wł/wy funkcji. Hasła silne opatrzone o litery, cyfry i znaki specjalne. Możliwość przypisania w BIOS numeru nadawanego przez Administratora.
Bezpieczeństwo	System diagnostyczny z graficzny interfejsem dostępny z poziomu BIOS lub menu BOOT'owania umożliwiający użytkownikowi przeprowadzenie wstępnej diagnostyki awarii poprzez przetestowanie: procesora, pamięci RAM, dysku, płyty głównej i wyświetlacza. Pełna funkcjonalność systemu diagnostycznego musi być dostępna również w przypadku braku lub uszkodzenia oraz sformatowania dysku twardego, braku dostępu do sieci LAN i internetu oraz nie może być realizowana przez narzędzia zewnętrzne podłączane do komputera (np. pamięć USB flash]. Dedykowany układ szyfrujący TPM 2.0 Złącze na linkę zabezpieczającą przed kradzieżą.
Certyfikaty	Certyfikat ISO 9001 dla producenta sprzętu (załączyć do oferty) Certyfikat ISO 50001 dla producenta sprzętu (załączyć do oferty) Deklaracja zgodności CE (załączyć do oferty) Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki.
System operacyjny	Zainstalowany system operacyjny Windows 11 Professional z możliwością downgrade'u do Win 10 Pro
Wymagania dodatkowe	Wbudowane porty i złącza: HDMI 1.4, RJ-45 (karta sieciowa wbudowana), min. 3xUSB w tym min. 2 port USB 3.2 gen1 typ-A, czytnik kart SD 3.0, współdzielone złącze słuchawkowe stereo i złącze mikrofonowe, złącze zasilania (zasilacz nie może zajmować portów USB) Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN 802.11AC, moduł bluetooth 4.1 Klawiatura z wbudowanym podświetleniem (układ US - QWERTY) z wydzieloną klawiaturą numeryczną, touchpad z strefą przewijania w pionie, poziomie wraz z obsługą gestów.
Dodatkowe oprogramowanie	Dostarczone i zainstalowane w środowisku systemu operacyjnego aplikacja zapewniająca bezproblemową integrację bezprzewodową między smartfonami i komputerem. Aplikacja wspierająca zgodna z systemami iOS oraz Android 6 lub nowszy. Opatrzona w funkcjonalności: - Inicjowanie i odbieranie połączeń telefonicznych przez głośniki i mikrofon w komputerze - Uzyskanie dostępu do kompletnej książki telefonicznej poprzez komputer - Wysyłanie i odbieranie wiadomości tekstowych za pomocą klawiatury, myszy i ekranu dotykowego komputera. - bezprzewodowo: przeciągnij i upuść zdjęcia, filmy, muzykę i dokumenty między

	komputerem a smartfonem z systemem Android lub iOS. - tworzenie kopi lustrzanej ekranu telefonu z systemem Android lub iOS na komputerze i korzystanie z dowolnych aplikacji za pomocą klawiatury, myszy i ekranu dotykowego komputera
Warunki gwarancji	3-letnia gwarancja producenta świadczona na miejscu u klienta. Czas reakcji serwisu - do końca następnego dnia roboczego. Dedykowany portal producenta do zgłaszania awarii lub usterek, możliwość samodzielnego zamawiania zamiennych komponentów oraz sprawdzenie okresu gwarancji, fabrycznej konfiguracji. Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.

2. Pakiet biurowy – 46 szt.

Oprogramowanie biurowe musi być nieużywane, nieaktywowane nigdy wcześniej na innym urządzeniu oraz pochodzić z legalnego źródła. Licencja na oprogramowanie biurowe musi być nieograniczona w czasie, pozwalać na wielokrotne instalowanie na oferowanym sprzęcie bez konieczności kontaktowania się przez Zamawiającego z producentem oprogramowania. Oprogramowanie powinno posiadać certyfikat autentyczności lub unikalny kod aktywacyjny. Zamawiający zastrzega sobie prawo do sprawdzenia legalności licencji u producenta oprogramowania. Zamawiający wymaga dostarczenia oprogramowania biurowego przeznaczonego dla użytku domowego oraz szkół.

Pakiet biurowy musi spełniać następujące wymagania:
1. Wymagania ogólne dla pakietu:
a. możliwość automatycznej instalacji komponentów (przy użyciu instalatora systemowego),
b. możliwość zdalnej instalacji komponentów,
c. możliwość prowadzenia dyskusji oraz subskrypcji dokumentów w sieci z automatycznym powiadomieniem o zmianach w dokumentach, oraz publikowanie dokumentów wprost z komponentów pakietu np. arkusza kalkulacyjnego,
d. możliwość nadawania uprawnień do modyfikacji i formatowania dokumentów lub ich fragmentów,
e. automatyczne wyróżnianie i aktywowanie hyperlinków w dokumentach podczas edycji i odczytu,
f. możliwość automatycznego odzyskiwania dokumentów w wypadku odcięcia dopływu prądu,
g. prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach:.doc, .docx, xls,.xlsx, ppt, .pptx, .pps, .ppsx, w tym obsługa formatowania, wykonywanie i edycję makr oraz kodu zapisanego w języku Visual Basic for Application w plikach xls, xlsx, formuł, formularzy w plikach wytworzonych w MS Office 2003, MS Office 2007, MS Office 2010, MS Office 2013, MS Office 2016 bez utraty danych oraz bez konieczności reformatowania dokumentów,
h. prawidłowe otwieranie i zapisywanie plików o formatach doc, docx, xls, xlsx, .ppt, pptx. .pps, .ppsx bez utraty parametrów i cech użytkowych zachowane wszelkie formatowanie, umiejscowienie tekstów, liczb, obrazków, wykresów, odstępy między tymi obiektami i kolorów, działające makra,
i. wszystkie komponenty oferowanego pakietu biurowego (edytor, arkusz, klient poczty, kalendarz oraz program do prezentacji) muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzanie i wymiana danych), posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi,
j. poprawna praca w systemach operacyjnych rodziny Microsoft,
k. zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu.

2. Dostępność pakietu w wersjach 32-bit oraz 64-bit,
3. Wymagania odnośnie interfejsu użytkownika:
a. Pełna polska wersja językowa interfejsu użytkownika.
4. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, spełniając następujące wymagania:
a. pozwala zapisywać dokumenty w formacie XML,
b. posiada kompletny i publicznie dostępny opis formatu,
c. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526).
5. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
6. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
7. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
a. Edytor tekstów,
b. Arkusz kalkulacyjny,
c. Narzędzie do przygotowywania i prowadzenia prezentacji,
d. Narzędzie do zarządzania informacją (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
e. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia.

3. Oprogramowanie – ochrona stacji roboczych - 46 szt.

1. Pełne wsparcie dla systemu Windows 10/Windows 11.
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim.
4. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
5. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim oraz angielskim.
6. **Czas trwania licencji: min. 2 lata**

Ochrona antywirusowa i antyspyware
6. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
7. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
8. Wbudowana technologia do ochrony przed rootkitami.
9. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
10. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
11. Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.
12. System ma posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
13. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
14. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
15. Możliwość skanowania dysków sieciowych i dysków przenośnych.
16. Skanowanie plików spakowanych i skompresowanych.

17. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
18. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
19. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
20. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
21. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
22. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
23. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
24. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
25. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
26. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
27. 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).
28. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
29. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
30. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
31. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
32. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
33. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
34. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
35. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
36. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
37. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
38. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
39. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
40. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
41. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.

42. 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
43. Możliwość automatycznego wysyłania nowych do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
44. Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
45. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
46. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
47. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
48. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
49. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
50. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
51. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
52. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
53. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
54. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
55. Program ma umożliwiać 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.
56. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
57. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
58. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
59. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
60. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
61. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
62. 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 program 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 program 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 program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

63. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
64. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
65. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
66. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
67. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, 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.
68. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.
69. Program ma posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
70. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
71. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
72. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
73. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
74. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
75. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
76. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.
77. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
78. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli rodzicielskiej i kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
79. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
80. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
81. Możliwość podejrzenia informacji o licencji, która znajduje się w programie.
82. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.

83. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
84. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
85. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
86. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść".
87. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
88. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
89. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
90. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.
91. Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

Ochrona przed spamem

92. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
93. Program ma umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
94. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
95. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
96. Możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
97. Możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
98. Możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
99. Program ma domyślnie współpracować z folderem „Wiadomości-śmieci", dostępnym w programie Microsoft Outlook.
100. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana"
101. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana".
102. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall)

103. Zapora osobista ma pracować w jednym z czterech trybów:
• tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
• tryb interaktywny – program pyta się o każde nowo nawiązywane połączenie,
• tryb oparty na regułach – program blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
• tryb uczenia się – program automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
104. Program musi oceniać reguły zapory systemu Windows.
105. Możliwość tworzenia list sieci zaufanych.

106. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
107. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.
108. Możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
109. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
110. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
111. Wykrywanie modyfikacji w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.
112. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
113. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
114. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
115. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
116. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.
117. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
118. Program musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów:
• z aplikacją lokalną, którą administrator wskazuje z listy,
• z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.

Kontrola rodzicielska
1. Aplikacja musi być wyposażona w zintegrowany moduł kontroli rodzicielskiej.
2. Moduł Kontroli rodzicielskiej musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane reguły filtrowania.
3. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
4. Dla kont użytkowników musi istnieć możliwość przypisania gotowych profili filtrowania kategorii.
5. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
6. Podstawowe kategorie, w jakie aplikacja musi być co najmniej wyposażona to: Osoby dorosłe, Agresywne, Alkohol i wyroby tytoniowe, Ukrywające tożsamość, Sztuka, Motoryzacja, Biznes i praca, Czaty i sieci społecznościowe, komunikacja, Działalność przestępcza, Oświata, Rodzina i wychowanie dzieci, Moda, Finanse, Żywność i napoje, Zdrowie, Hobby i zainteresowania, Dzieci, Styl życia, Aktualności, Zwierzęta domowe, Zagadnienia społeczne, polityczne i prawne, Nieruchomości, Religia, Nauka, Edukacja seksualna, Zakupy, Sport, Technologie, Podróże
7. Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta.
8. Dla poszczególnych kont użytkownik ma posiadać możliwość utworzenia wyjątków dla konkretnych adresów url, które mogą być wyświetlone nawet w przypadku, gdy dany adres znajduje się w którejkolwiek z blokowanych kategorii.
9. Aplikacja musi być wyposażona w moduł logowania zablokowanych stron oraz kategorii niezależnie od zalogowanego użytkownika.
10. Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli rodzicielskiej.

Ochrona Bankowości elektronicznej

11. Aplikacja musi być wyposażona w moduł ochrony bankowości internetowej.
12. Przeglądarka powinna automatycznie szyfrować wszelkie dane wpisywane przez Użytkownika w formularzach internetowych. Szyfrowanie powinno odbywać się na poziomie odczytu znaków wpisywanych z klawiatury.
13. Producent musi zapewniać aktualizację bazy witryn, dla których automatycznie będzie uruchomiony moduł ochrony bankowości internetowej.
14. W momencie wejścia na stronę, która znajduje się na liście producenta Użytkownik musi mieć możliwość wyboru czy chce uruchomić bezpieczną przeglądarkę.
15. Użytkownik w każdym czasie musi mieć możliwość ręcznego uruchomienia przeglądarki w trybie zabezpieczonym modułem ochrony bankowości elektronicznej dla dowolnego adresu URL.
16. Program musi oferować możliwość zapamiętania wyboru dla danej witryny lub też wybrania opcji pytania za każdym razem.
17. W momencie wyświetlenia witryny wymagającej bezpiecznego połączenia użytkownik musi mieć możliwość wyboru czy witryna ma być otwarta za pomocą standardowej czy też zabezpieczonej przeglądarki.
18. Praca w trybie bezpiecznym musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na pasku przeglądarki.

Monitor sieci domowej

19. Aplikacja ma posiadać moduł skanujący sieć domową, do której podłączony jest użytkownik, wyświetlając obecnie podłączone urządzenia sieciowe oraz sygnalizować nowo podłączane.
20. Wyświetlane hosty widoczne są pod ich nazwą NETBIOS, adresem IP oraz adresem MAC. Wraz z tymi informacjami wyświetlane muszą być informacje na temat ostatniego wykrycia hosta.
21. Wyświetlana nazwa hosta może być modyfikowana przez użytkownika.
22. Aplikacja musi być wyposażona w mechanizm umożliwiający tworzenie reguł dla ostatnio zablokowanej komunikacji, użytkownik musi mieć możliwość wyświetlania komunikacji, jaka była blokowana w ostatnim czasie (co najmniej ostanie 5,15,60 minut).
23. Użytkownik ma możliwość otwarcia interfejsu logowania się do swojego urządzenia brzegowego (routera itp.) poprzez link umieszczony w menu aplikacji.
24. Moduł ochrony sieci musi mieć możliwość przeprowadzenia audytu zabezpieczeń routera znajdującego się w sieci użytkownika.
25. System skanowania routera musi mieć możliwość wykrycia co najmniej otwartych portów sieciowych, zabezpieczenia konfiguracji urządzenia za pomocą domyślnych lub słabych haseł.
26. Moduł ochrony sieci domowej wykonujący skanowanie pod kątem otwartych portów powinien sprawdzać co najmniej porty 80, 443, 139, 445, 21, 22, 23.
27. Moduł musi wykrywać również urządzenia podłączone w sieci domowej należące do grupy produktów „Internet of Things".
28. Moduł ten musi mieć możliwość wykrycia, czy urządzenie pracuje w sieci publicznej czy lokalnej. W przypadku sieci publicznej program musi wyświetlić ostrzeżenie użytkownikowi o ryzyku skanowania w takim trybie.

Ochrona kamery internetowej

29. Aplikacja ma umożliwiać kontrolę użycia kamery internetowej przez procesy znajdujące się w systemie jak i inne aplikacje.
30. W przypadku próby użycia kamery przez aplikację lub proces systemowy, użytkownikowi musi wyświetlić się stosowny komunikat ostrzegawczy.
31. Wykrycie próby użycia kamery musi dać użytkownikowi możliwość zezwolenia lub blokady takiej czynności.
32. Użytkownik może utworzyć listę aplikacji, które będą miały dostęp do kamery. Analogiczna lista musi zostać utworzona dla aplikacji, dla których wykonywana będzie blokada.

Ochrona antykradzieżowa

33. Program musi posiadać moduł umożliwiający powiązanie zainstalowanego w systemie pakietu ochrony z kontem utworzonym na dedykowanym serwisie online dostępnym za pomocą przeglądarki internetowej na serwerach producenta.
34. Po zalogowaniu do swojego indywidualnego konta na portalu producenta użytkownik powinien mieć wylistowane urządzenia, z którymi jest to konto powiązane.
35. Logowanie do portalu za pomocą przeglądarki internetowej musi odbywać się poprzez zabezpieczoną komunikację HTTPS.
36. Portal musi posiadać polski interfejs.
37. Użytkownik z poziomu swojego konta musi posiadać możliwość wykonania testu na widocznym w portalu swoim komputerze w celu weryfikacji poprawności działania modułu antykradzieżowego.
38. Wyzwolenie zadania testu musi wymagać potwierdzenia jego wykonania od strony użytkownika urządzenia, na którym test ma być wykonany.
39. W trakcie testu mechanizmy wbudowane w pakiet antywirusowy muszą zebrać co najmniej informację o: lokalizacji testowanego komputera (jeśli jest ona dostępna) – urządzenie powinno być wskazane na mapie w postaci graficznej, wykonać screenshoot'a pulpitu oraz wykonać zdjęcie za pomocą wbudowanej w komputer kamery (jeśli jest dostępna) i zebrać informację o adresie IP, z jakiego łączy się testowany komputer.
40. Zebrane podczas testów informacje muszą być widoczne dla zalogowanego na portalu użytkownika.
41. W przypadku kradzieży lub zagubienia urządzenia, Użytkownik musi posiadać możliwość określenia swojego urządzenia jako brakującego.
42. W momencie, gdy urządzenie zostanie określone jako brakujące, automatycznie musi zostać przesłane na nie zadanie aktywacji dedykowanego konta systemowego z ograniczeniami, oraz wymuszenie restartu systemu Windows.
43. Po restarcie komputera musi istnieć możliwość zalogowania się jedynie do konta z ograniczeniami utworzonego przez mechanizmy auto ochrony, pozostałe konta systemowe mają być nieaktywne.
44. Mechanizm antykradzieżowy w momencie aktywacji ma automatycznie tworzyć zdjęcia przy wykorzystaniu wbudowanej w urządzenie kamery (jeśli dostępna), zapisywać obraz pulpitu, zbierać informacje odnośnie lokalizacji urządzenia oraz wykorzystywanych adresów IP.
45. Zebrane informacje mają zostać przesłane na konto użytkownika utworzone na portalu producenta.
46. W przypadku braku połączenia z siecią Internet, w/w informacje maja być zbierane i przesłane do portalu w momencie, gdy urządzenie będzie posiadało aktywne połączenie z siecią Internet.
47. Zalogowany do konta na portalu producenta użytkownik musi posiadać możliwość zdalnego wyświetlenia na brakującym urządzeniu dowolnego komunikatu zawierającego tekst i obraz.
48. Z poziomu portalu, użytkownik musi mieć dostęp do danych historycznych wcześniej zebranych podczas testów lub w momencie określenia urządzenia jako brakującego.
49. Użytkownik musi posiadać opcję usunięcia swojego konta z serwerów producenta wraz z informacjami tam się znajdującymi.

Menedżer licencji

50. Interfejs menedżera licencji musi być dostępny z poziomu strony WWW.
51. Dostęp do witryny musi być zabezpieczony z pomocą SSL.
52. Interfejs webowy musi być dostępny w języku polskim.
53. Interfejs www musi posiadać możliwość dodania więcej niż jednej licencji.
54. Produkt zabezpieczający musi posiadać możliwość aktywacji przy pomocy danych logowania menedżera licencji.
55. Komputer po aktywacji musi się zgłaszać do menedżera licencji za pomocą nazwy NETBIOS.
56. Menedżer musi pokazywać liczbę wykorzystanych i dostępnych licencji.
57. Musi być możliwość zmiany nazwy komputera na stornie www po dokonaniu aktywacji .
58. Dezaktywacja licencji musi być dostępna bezpośrednio z interfejsu www.
59. Przy usuwaniu licencji z interfejsu www musi być dostępna opcja dezaktywacji wszystkich stacji.