Zatwierdzam
Burmistrz Miastka
Jerzy Wójtowicz
(-)

Miastko, dnia 07.11.2024 r.

S p e c y f i k a c j a
Warunków Zamówienia

Zamawiający : **Gmina Miastko**
pow. bytowski, woj. pomorskie

Przedmiot zamówienia:
„ Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko.”

Tryb postępowania: **Podstawowy**

ogłoszony w Biuletynie Zamówień Publicznych
Nr ogłoszenia: 2024/BZP 00586137
Data zamieszczenia: 08.11.2024 r.

Miastko, listopad 2024 r.

Spis treści

I. Zamawiający

Gmina Miastko
Adres: ul. Grunwaldzka 1, 77 - 200 Miastko tel. (059) 857-07 02
Adres poczty elektronicznej: monika.maksymow@um.miastko.pl
Adres strony internetowej prowadzonego postępowania: https://platformazakupowa.pl/um_miastko

II. Adres strony internetowej, na której udostępniane będą zmiany i wyjaśnienia treści swz oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia

Zmiany i wyjaśnienia treści niniejszej specyfikacji warunków zamówienia zwaną także „swz" oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia będą udostępniane na stronie internetowej:
https://platformazakupowa.pl/um_miastko

III. Tryb udzielenia zamówienia

Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym, na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320), zwanej dalej także „Pzp" oraz niniejszej swz o wartości zamówienia mniejszej niż progi unijne określone w przepisach wydanych na podstawie art. 3 ust. 3 Pzp.

IV. Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest rozbudowa infrastruktury informatycznej urzędu polegająca na dostawie sprzętu wraz z instalacją, montażem i przeniesieniem danych z obecnej sieci informatycznej oraz wdrożenie oprogramowania do zarządzania siecią IT wraz z konfiguracją sieci VLAN oraz dostawa oprogramowania do monitorowania infrastruktury sieci informatycznej i urządzeń dla jednostki podległej oraz dostawa usług chmurowych w ramach zabezpieczenia poczty i stron internetowych Gminy.
2. Przedmiot zamówienia musi być dostarczany, wdrożony i zainstalowany w całości do siedziby Zamawiającego.
3. **Zamawiający wymaga załączenia do Formularza ofertowego wykazu oferowanego sprzętu wraz ze szczegółowym opisem technicznym – cz. I- załącznik 2a do swz/ Wykaz oferowanego oprogramowania wraz ze szczegółowym opisem technicznym – cz. II – załącznik 2b do swz** - w taki sposób aby Zamawiający mógł jednoznacznie określić szczególne cechy produktu oraz wymagane prawem certyfikaty, deklaracje zgodności CE, instrukcje obsługi sprzętu, dokumenty gwarancyjne, celem sprawdzenia zgodności oferowanego produktu.
4. Jeżeli w opisie przedmiotu zamówienia wskazano jakikolwiek znak towarowy, patent lub pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę – należy przyjąć, że Zamawiający podał taki opis w celu określenia **minimalnych parametrów**, jakim muszą odpowiadać produkty, aby spełnić wymagania stawiane przez Zamawiającego i stanowią one wyłącznie wzorzec jakościowy przedmiotu zamówienia, a nie wskazanie na konkretny wyrób danego producenta. Zgodnie z art. 99 ust. 5 ustawy Prawo zamówień publicznych. Zamawiający dopuszcza możliwość złożenia oferty równoważnej, jednak pod warunkiem, że zaproponowany przez Wykonawcę produkt równoważny będzie spełniał minimum wymogów tej samej klasy jakiej oczekuje Zamawiający, tzn. będzie odpowiadał wymaganiom opisanym przez Zamawiającego w SWZ. Asortyment zaproponowany jako równoważny nie może odbiegać jakością, standardem, parametrami technicznymi od założonych przez Zamawiającego. Za asortyment równoważny Zamawiający uzna ten, który posiada te same lub lepsze od opisanych w SWZ parametry techniczne i jakościowe, a jego zastosowanie w żaden sposób nie wpłynie na prawidłowe funkcjonowanie infrastruktury informatycznej Zamawiającego. Wykonawca, który powołuje się na rozwiązania równoważne jest zobowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. Ciężar dowodowy w zakresie udowodnienia równoważności zaoferowanych rozwiązań z rozwiązaniami opisanymi poprzez wskazanie przykładowego znaku towarowego, patentu lub pochodzenia, spoczywa na Wykonawcy, składającym ofertę równoważną. Wykonawcy powinni oznaczyć, której części oraz którego punktu tabeli **załącznika nr 2a do SWZ - Wykaz oferowanego sprzętu wraz z szczegółowym opisem technicznym/2b Wykaz oferowanego oprogramowania wraz z szczegółowym opisem technicznym** dokumenty dotyczą. Jeżeli w prospektach brak opisu danego wymogu, dopuszcza się załączenie do oferty innych dokumentów, w

których Zamawiający będzie w stanie zweryfikować zgodność opisu danego wymogu lub oświadczenie producenta. Zamawiający dopuszcza także oświadczenie własne wykonawcy w przypadku gdy dany parametr nie można potwierdzić w inny sposób.

5. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca przeprowadzi zgodnie z zapisami niniejszego OPZ w uzgodnieniu z Zamawiającym, zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów informatycznych oraz najlepszymi praktykami w ich realizacji.
6. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, zapisami OPZ oraz Umowy.
7. Wykonawca musi dostarczyć wszelkie urządzenia i elementy, które są niezbędne do prawidłowego funkcjonowania całości. W przypadku, gdy w trakcie realizacji Przedmiotu Zamówienia okaże się, że brakuje jakiegokolwiek urządzenia, elementu i/lub licencji, którego brak spowoduje nieprawidłowe funkcjonowanie całości Przedmiotu Zamówienia, Wykonawca dostarczy je na własny koszt.
8. Wszelkie dostarczane urządzenia:
   1) muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta;
   2) nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych;
   3) nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta;
   4) elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta;
   5) urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta;
   6) urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta;
   7) do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.
9. Nomenklatura

   9.1. Kody CPV:

   Cz. I zamówienia:

   80000000-4 Usługi edukacyjne i szkoleniowe
   80550000-4 Usługi szkolenia w dziedzinie bezpieczeństwa
   48821000-9 Serwery sieciowe
   79417000-0 Usługi doradcze w zakresie bezpieczeństwa
   48000000-8 Pakiety oprogramowania i systemy informatyczne
   35100000-5 Urządzenia awaryjne i zabezpieczające
   32420000-3 Urządzenia sieciowe
   30200000-1 Urządzenia komputerowe
   31122000-7 Jednostki prądotwórcze
   32422000-7 Elementy składowe sieci
   72263000-6 Usługi wdrażania oprogramowania
   72541000-9 Usługi rozbudowy sprzętu komputerowego

   Cz. II zamówienia :

   72317000-0 Usługi przechowywania danych
   48000000-8 Pakiety oprogramowania i systemy informatyczne.
10. Przedmiot zamówienia jest dofinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02.-CS.01-001/23. Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/2110/FERC.02.02-CS.01-001/23/2024.

V. Opis części zamówienia

1. Przedmiot zamówienia podzielony jest na dwie części:

1) Część nr 1 obejmuje rozbudowę infrastruktury informatycznej urzędu opartą na dostawie sprzętu wraz z instalacją, montażem i przeniesieniem danych z obecnej sieci informatycznej oraz wdrożenie oprogramowania do zarządzania siecią IT wraz z konfiguracją sieci VLAN. Wykonawca jest zobowiązany

do sporządzenia dokumentacji z przeprowadzonego wdrożenia oraz przeprowadzenia szkoleń specjalistycznych z zastosowanych rozwiązań. **Szczegółowe opisy minimalnych parametrów technicznych urządzeń, oprogramowania i szkoleń w ramach zadania dla części nr 1 zostały opisane w rozdziale II Opisu przedmiotu zamówienia – załącznik nr 1 swz:**

Poz. OPZ	**Opis**	**Ilość sztuk/kpl**
Rozdział	**Rodzaj zamawianego asortymentu**	
II.1.1	Serwer I - Dostawa, instalacja i wdrożenie serwerów w celu utworzenia klastra pracy awaryjnej urzędu. Konfiguracja klastra	3 szt.
II.1.2	Serwer II - Dostawa serwera	1 szt.
II.1.3	Oprogramowanie i licencje do serwerów	Zgodnie z opisem
II.1.4	Macierz - Dostawa, instalacja, konfiguracja macierzy z klastrem pracy awaryjnej, Przeniesienie danych z dotychczasowych nośników.	1 szt.
II.1.5	Dostawa i wdrożenie oprogramowania do wykonywania kopii zapasowych wraz z usługą chmurową	1 szt.
II.1.6	Wdrożenie oprogramowania do zarządzania infrastrukturą IT na 80 licencji	1 szt.
II.1.7	Wdrożenie usług domeny do zarzadzania siecią i zasobami komputerowymi	1 szt.
II.1.8	Przełącznik dystrybucyjny L3	1 szt.
II.1.9	Przełączniki sieciowe - Dostawa i wdrożenie zarządzalnych przełączników sieciowych do utworzenia rdzenia sieci LAN	6 szt.
II.1.10	Dostawa, instalacja oraz podłączenie zasilacza awaryjnego UPS z kartą SNMP	1 szt.
II.1.11	Dostawa wraz z montażem i uruchomieniem dysków 12TB przeznaczonych do wykonywania kopii zapasowych	5 szt.
II.1.12	Szkolenie ASI tworzenie i administracja sieci VLAN	1 szt.
II.1.13	Szkolenie ASI tworzenie i administracja serwerami Windows	1 szt.
II.1.14	Szkolenie ASI z domeny do zarzadzania siecią i zasobami komputerowymi	1 szt.
II.1.15	Szkolenie ASI Budowa klastra Hyper-V	1 szt.
II.1.16	Szkolenie z oprogramowania do zarządzania infrastrukturą IT	1 szt.

Tabela nr 1 – Spis urządzeń dla części nr 1

2) Część nr 2 obejmuje dostawę oprogramowania do monitorowania infrastrukturą sieci informatycznej i urządzeń dla jednostki podległej oraz dostawę usług chmurowych w ramach zabezpieczenia poczty i stron internetowych Gminy. **Szczegółowe opisy minimalnych parametrów technicznych urządzeń, oprogramowania i szkoleń w ramach zadania dla części nr. 2 zostały opisane w rozdziale II Opisu przedmiotu zamówienia – załącznik nr 1 swz**:

Poz. OPZ	**Opis**	**Ilość sztuk/kpl**
Rozdział	**Rodzaj zamawianego asortymentu**	
II.2.1	Oprogramowanie do zarządzania infrastrukturą IT na 31 licencji dla MOPS	1 szt.
II.2.2	Usługa zabezpieczenia poczty	1 szt.
II.2.3	Usługa zabezpieczenia serwisu www na 24 miesiące	1 szt.

Tabela nr 2 – Spis urządzeń dla części nr 2

VI. Liczba części zamówienia, na którą wykonawca może złożyć ofertę

Zamawiający dopuszcza możliwość składania ofert częściowych.

VII. Informacja dotycząca ofert wariantowych

Zamawiający nie dopuszcza składania ofert wariantowych.

VIII. Wymagania dotyczące wadium

1. Zamawiający na podstawie art. 97 ust. 1 Pzp żąda od wykonawców ubiegających się o udzielenie zamówienia wniesienia wadium dla każdej wskazanej w swz części, na którą zamierza złożyć ofertę w kwocie: **5.700 zł** słownie: pięć tysięcy siedemset 00/100 złotych. – **dotyczy części I postępowania.**
2. Wykonawca ubiegający się o udzielenie zamówienia zobowiązany jest do wniesienia wadium przed upływem terminu składania ofert.
3. Wadium może być wnoszone według wyboru wykonawcy w jednej lub kilku następujących formach:
   1) w pieniądzu;
   2) gwarancjach bankowych;
   3) gwarancjach ubezpieczeniowych;
   4) poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz.U. z 2019 r. poz. 310, 836 i 1572).
4. Wadium wnoszone w pieniądzu musi być wpłacone przelewem na rachunek bankowy zamawiającego - **PKO Bank Polski SA 17 1020 2791 0000 7702 0258 4803.** Wniesione w ten sposób wadium będzie **skuteczne** jeżeli w podanym terminie znajdzie się na rachunku bankowym zamawiającego. W przeciwnym przypadku wykonawca zostanie wykluczony z postępowania. Dlatego też należy dochować należytej staranności aby nie dopuścić do uchybienia wskazanego terminu.
   Uwaga: Niedopuszczalna jest forma gotówkowej wpłaty w kasie Urzędu Miejskiego w Miastku.
5. Jeżeli wadium jest wnoszone w formie gwarancji lub poręczenia, o którym mowa w poz. 3 pkt 2 - 4 swz, wykonawca przekazuje zamawiającemu oryginał gwarancji lub poręczenia, **w postaci elektronicznej**.
6. Z treści dokumentów stanowiących wniesione wadium w formie gwarancji lub poręczenia, o którym mowa w poz. 3 pkt 2- 4 swz, musi jednoznacznie wynikać jaki jest sposób reprezentacji Gwaranta/Poręczyciela. Wystawiony dokument musi być podpisany przez upoważnionego (upełnomocnionego) przedstawiciela instytucji wystawiającej. Z treści wystawionego dokumentu winno wynikać bezwarunkowe, na każde pisemne żądanie zgłoszone przez zamawiającego w okresie związania ofertą, zobowiązuje Gwaranta/Poręczyciela do wypłaty zamawiającemu pełnej kwoty wadium w okolicznościach określonych w art. 98 ust. 6 Pzp.
7. Wniesienie wadium w innej **nieakceptowanej formie** spowoduje odrzucenie oferty.
8. Zwrot wadium

8.1. Zamawiający zwróci wadium w okolicznościach i na zasadach określonych w art. 98 ust. 1-5 Pzp;.

8.2. Wadium wniesione w pieniądzu zamawiający zwraca wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszty jego prowadzenia oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy wskazany przez wykonawcę;

9. Zatrzymanie wadium

9.1. Zamawiający zatrzyma wadium w okolicznościach i na zasadach określonych w art. 98 ust. 6 Pzp.

IX. Informacja o przewidzianych zamówieniach, o których mowa w art. 214 ust. 1 pkt. 7- 8 Pzp

Zamawiający informuje, że przewiduje możliwości udzielenia zamówień, o których mowa w art. 214 ust. 1 pkt 7 i 8 Pzp.

X. Informacja dotycząca przeprowadzenia przez wykonawcę wizji lokalnej

Zamawiający nie wymaga przeprowadzenia wizji lokalnej.

XI. Informacja dotycząca walut obcych, w jakich mogą być prowadzone rozliczenia między zamawiającym a wykonawcą

Zamawiający nie przewiduje rozliczeń z wykonawcą w walucie obcej.

XII. Informacje dotyczące zwrotu kosztów udziału w postępowaniu

Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

XIII. Termin wykonania zamówienia

Wykonawca zobowiązany jest zrealizować przedmiot zamówienia w terminie:

1) Cz. I - **90 dni** od dnia zawarcia umowy;
2) Cz.II – **30 dni** od zawarcia umowy.

XIV. Informacja o warunkach udziału w postępowaniu

1. O udzielenie zamówienia publicznego mogą ubiegać się wykonawcy, którzy:

1) nie podlegają wykluczeniu na zasadach określonych w Rozdziale XV SWZ;
2) spełniają warunki udziału w postępowaniu.

2. Zamawiający wymaga wykazania przez wykonawcę spełnienia warunków określonych w art. 112 ust. 2 Pzp dotyczących:
   3) zdolności do występowania w obrocie gospodarczym:
   Zamawiający nie stawia warunku w powyższym zakresie;
   4) uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:
   Zamawiający nie stawia warunku w powyższym zakresie;
   5) sytuacji ekonomicznej lub finansowej
   Zamawiający nie stawia warunku w powyższym zakresie;
   6) zdolności technicznej lub zawodowej
   O zamówienie może ubiegać się Wykonawca, który:
   Cz.I
   a) posiada wiedzę i doświadczenie, co należycie udokumentuje, tj. wykaże, że w okresie ostatnich 3 lat przed upływem składania ofert, a jeżeli okres prowadzenia działalności jest krótszy w tym okresie, należycie wykonał:
      - minimum 2 dostawy systemów z zakresu cyberbezpieczeństwa o zbliżonym charakterze jak przedmiot zamówienia, tj. dostawie sprzętu wraz z instalacją, montażem oraz wdrożeniem oprogramowania do zarządzania siecią IT wraz z konfiguracją sieci VLAN na kwotę min 300 000 brutto każda (słownie: trzysta tysięcy złotych 00/100)
   b) dysponuje kadrą posiadającą doświadczenie zawodowe gwarantujące należyte wykonanie zamówienia tj. dysponuje minimum 1 osobą uczestniczącą w realizacji zamówienia, która:
      - posiada co najmniej 2-letnim doświadczenie zawodowe (praktyczne i/lub dydaktyczne) w zakresie wystąpień/szkoleń/prelekcji o tematyce bezpieczeństwa informacji
        oraz
      - w okresie ostatnich 3 lat przed upływem składania ofert, a jeżeli okres prowadzenia działalności jest krótszy w tym okresie, przeprowadziła minimum 2 wystąpienia/szkolenia/prelekcje o związanych z tematyką bezpieczeństwa informacji.

   Cz.II
   c) posiada wiedzę i doświadczenie, co należycie udokumentuje, tj. wykaże, że w okresie ostatnich 3 lat przed upływem składania ofert, a jeżeli okres prowadzenia działalności jest krótszy w tym okresie, należycie wykonał:
      - minimum 2 dostawy o zbliżonym charakterze jak przedmiot zamówienia tj. dostawy oprogramowania do monitorowania infrastruktury sieci informatycznej i urządzeń oraz usług chmurowych w ramach zabezpieczenia poczty i stron internetowych na kwotę min **20.000 zł** brutto każda (słownie: dwadzieścia tysięcy złotych 00/100).
3. Ocena spełnienia wymaganego warunku zostanie przeprowadzona w oparciu o informacje zawarte w dokumentach lub oświadczeniach wyszczególnionych w rozdziale XVI i odpowiednio w wykazie, który Wykonawca zobowiązany jest przedłożyć zamawiającemu w celu potwierdzenia spełniania tego warunku zgodnie z opisem w w/w części oraz załącznikiem nr 7 do SWZ. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia stosownie do art. 58 ustawy Pzp (np. na podstawie umowy konsorcjalnej) opisany warunek powinny spełniać wspólnie.
4. Zamawiający informuje, że nie zastrzega osobistego wykonania przez Wykonawcę kluczowych części zamówienia. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcom. Wykonawca jest zobowiązany wskazać w Formularzu oferty części zamówienia, której wykonanie powierzone zostanie podwykonawcom i podać firmy podwykonawców, jeśli są już znane. Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się, na zasadach określonych w art. 118 ust. 1 ustawy Pzp, w celu wykazania spełniania warunków udziału w postępowaniu, Wykonawca jest obowiązany wykazać Zamawiającemu, że proponowany inny Podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż Podwykonawca, na którego zasoby Wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia.
5. Zamawiający, w stosunku do Wykonawców wspólnie ubiegających się o udzielenie zamówienia, w odniesieniu do warunków dotyczącego zdolności technicznej lub zawodowej – dopuszcza łączne spełnienie warunku przez Wykonawców.

6. Zamawiający może na każdym etapie postępowania uznać, że Wykonawca nie posiada wymaganych zdolności, jeżeli posiadanie przez Wykonawcę sprzecznych interesów, w szczególności zaangażowanie zasobów technicznych lub zawodowych Wykonawcy w inne przedsięwzięcia gospodarcze Wykonawcy może mieć negatywny wpływ na realizację zamówienia.

XV. Podstawy wykluczenia z postępowania, o których mowa w art. 108 ust. 1 Pzp i art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspierania agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. poz. 835 z późn. zm.).

1. Na podstawie art. 108 ust. 1 Pzp z postępowania o udzielenie zamówienia wyklucza się, z zastrzeżeniem art. 110 ust. 2 Pzp, wykonawcę:

   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 (t.j. Dz. U. z 2024 r. poz. 1488) 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 (t.j. Dz. U. z 2024 r. poz. 930 z późn. zm.),
   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 (t.j. Dz. U. 2021 poz. 1745),
   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 dnia15 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 decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
4) wobec którego orzeczono zakaz ubiegania się 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 lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;
6) jeżeli, w przypadkach, o których mowa w art. 85 ust. 1 Pzp, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego Wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być

wyeliminowane w inny sposób niż przez wykluczenie Wykonawcy z udziału w postępowaniu o udzielenie zamówienia;

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

XVI. Informacje o oświadczeniach i dokumentach, jakie zobowiązani są dostarczyć Wykonawcy w celu potwierdzenia spełniania warunków udziału w postępowaniu oraz wykazania braku podstaw wykluczenia (podmiotowe środki dowodowe)

1. Do oferty wykonawca zobowiązany jest dołączyć :
   1) aktualne na dzień składania ofert świadczenie o spełnianiu warunków udziału w postępowaniu oraz braku podstaw do wykluczenia z postępowania składane na podstawie art. 125 ust. 1 Pzp - zgodnie z załącznikiem nr 3 i 4 do SWZ *(druk do wypełnienia lub wzorowania się).* Informacje zawarte w oświadczeniu stanowią wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu oraz spełniania warunków udziału w postępowaniu;
   2) wykaz oferowanego sprzętu wraz z szczegółowym opisem technicznym- cz. I – zał.2a/Wykaz oferowanego oprogramowania wraz z szczegółowym opisem technicznym-cz.II-zał. 2b.
   W przypadku złożenia oferty na obie części Wykonawca dołącza do oferty oba wykazy.
2. Zamawiający wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni od dnia wezwania, podmiotowych środków dowodowych, jeżeli wymagał ich złożenia w ogłoszeniu o zamówieniu lub dokumentach zamówienia, aktualnych na dzień złożenia następujących podmiotowych środków dowodowych:
   1) oświadczenie wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy, o braku przynależności do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2024 r. poz. 594 z późn. zm.) z innym wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej - załącznik nr 5 do swz;
   2) wykaz dostaw wykonanych w okresie 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy, w tym okresie, wraz z podaniem ich przedmiotu, dat wykonania i podmiotów na rzecz których dostawy zostały wykonane, z załączeniem dowodów określających czy te dostawy zostały wykonane należycie, przy czym dowodami, o których mowa są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy zostały wykonane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy. Ww. wykaz stanowi załącznik nr 8 do SWZ.
   3) Wykaz osób skierowanych do realizacji zamówienia odpowiedzialnych za przeprowadzenie szkoleń wraz z informacjami na temat ich doświadczenia i zrealizowanych w okresie 3 lat przed upływem terminu

składania ofert a jeżeli okres prowadzenia działalności jest krótszy przeprowadzonych wystąpień/szkoleń/prelekcje związanych z tematyką bezpieczeństwa informacji wraz z podaniem ich przedmiotu, dat wykonania i podmiotów na rzecz których usługi zostały wykonane, z załączeniem dowodów określających czy te usługi zostały wykonane należycie, przy czym dowodami, o których mowa są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy zostały wykonane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy. Ww. wykaz stanowi załącznik nr 9 do SWZ

Podmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia należy przekazać zamawiającemu przy użyciu środków komunikacji elektronicznej określonych w rozdziale XX SWZ, w zakresie i w sposób określony w Rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020r. poz. 2452).

XVII. Poleganie na zasobach innych podmiotów

1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
2. W odniesieniu do warunków dotyczących doświadczenia, wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają świadczenie do realizacji którego te zdolności są wymagane.
3. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa, wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
   Wzór oświadczenia stanowi załącznik nr 7 do SWZ.
4. Zamawiający ocenia, czy udostępniane wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe, pozwalają na wykazanie przez wykonawcę spełniania warunków udziału w postępowaniu, a także bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem wykonawcy.
5. Jeżeli zdolności techniczne lub zawodowe podmiotu udostępniającego zasoby nie potwierdzają spełniania przez wykonawcę, warunków udziału w postępowaniu lub zachodzą wobec tego podmiotu podstawy wykluczenia zamawiający żąda, aby wykonawca w terminie określonym przez zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.
6. **UWAGA:** Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.
7. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia wraz z oświadczeniami, o którym mowa w Rozdziale XVI. poz. 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, wzór oświadczenia stanowi załącznik nr 6 do swz.

XVIII. Informacja dla Wykonawców wspólnie ubiegających się o udzielenie zamówienia (spółki cywilne/konsorcja)

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo winno być załączone do oferty.
2. W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenia, o których mowa w Rozdziale XVI poz. 1 SWZ, składa każdy z wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
3. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika podział realizacji przedmiotu zamówienia przez poszczególnych wykonawców.

4. Oświadczenie i dokumenty potwierdzające brak podstaw do wykluczenia z postępowania składa każdy z wykonawców wspólnie ubiegających się o zamówienie.

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

1. Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do treści tej umowy, określone zostały w załączniku nr 10 do SWZ.

XX. 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, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje, przekazywane są elektronicznie za pośrednictwem platformazakupowa.pl (dalej jako „Platforma") pod adresem: **https://platformazakupowa.pl/um_miastko** i formularza **„Wyślij wiadomość do zamawiającego"** dostępnego na stronie dotyczącej danego postępowania **(nie dotyczy składania ofert).**
2. W sytuacjach awaryjnych np. w przypadku niedziałania Platformy, Zamawiający dopuszcza komunikację za pomocą poczty elektronicznej na adres: **sekretariat@um.miastko.pl (nie dotyczy składania ofert).**
3. Korzystanie z platformy zakupowej przez wykonawcę jest bezpłatne.
4. Wykonawca przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:
   1) akceptuje warunki korzystania z Platformy, określone w Regulaminie zamieszczonym na stronie internetowej pod linkiem w zakładce „Regulamin" oraz uznaje go za wiążący;
   2) zapoznał i stosuje się do Instrukcji składania ofert dostępnej pod adresem: https://drive.google.com/file/d/1Kd1DttbBeiNWt4q4slS4t76lZVKPbkyD/view
5. Zamawiający, zgodnie z Rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020 r. poz. 2452), określa niezbędne wymagania sprzętowo-aplikacyjne umożliwiające pracę na Platformie, tj.:
   1) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
   2) komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje,
   3) zainstalowana dowolna, inna przeglądarka internetowa niż Internet Explorer,
   4) włączona obsługa JavaScript,
   5) zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,
   6) Szyfrowanie na platformazakupowa.pl odbywa się za pomocą protokołu TLS 1.3.
   7) Oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.
6. Za datę przekazania składanych dokumentów, oświadczeń, wniosków (innych niż wnioski o dopuszczenie do udziału w postępowaniu), zawiadomień, zapytań oraz przekazywanie informacji uznaje się kliknięcie przycisku **„Wyślij wiadomość do zamawiającego"** po których pojawi się komunikat, że wiadomość została wysłana do Zamawiającego.
7. Zamawiający będzie przekazywał Wykonawcom informacje w formie elektronicznej za pośrednictwem Platformy. Informacje dotyczące odpowiedzi na pytania, zmiany specyfikacji, zmiany terminu składania i otwarcia ofert Zamawiający będzie zamieszczał na platformie w sekcji **„Komunikaty".** Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny Wykonawca, będzie przekazywana w formie elektronicznej za pośrednictwem Platformy do konkretnego Wykonawcy.
8. Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na Platformie przesłanych przez zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.
9. Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania z Platformy, w szczególności za sytuację, gdy zamawiający zapozna się z treścią oferty przed upływem terminu składania ofert (np. złożenie oferty w zakładce **„Wyślij wiadomość do zamawiającego").** Taka oferta zostanie uznana przez zamawiającego za ofertę handlową i nie będzie brana pod uwagę w

przedmiotowym postępowaniu ponieważ nie został spełniony obowiązek narzucony w art. 221 ustawy Pzp.

10. Zamawiający informuje, że instrukcje korzystania z Platformy dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści swz, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu platformazakupowa.pl znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje
11. Wykonawca może zwrócić się do zamawiającego z wnioskiem o wyjaśnienie treści swz.
12. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania odpowiednio ofert, pod warunkiem że wniosek o wyjaśnienie treści swz wpłynął do zamawiającego nie później niż na 4 dni przed upływem terminu składania odpowiednio ofert.
13. Jeżeli zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w ust. 12, przedłuża termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia ofert. W przypadku gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie, o którym mowa w ust. 12, zamawiający nie ma obowiązku udzielania wyjaśnień swz oraz obowiązku przedłużenia terminu składania ofert.
14. Przedłużenie terminu składania ofert, o których mowa w ust. 13, nie wpływa na bieg terminu składania wniosku o wyjaśnienie - treści swz.

XXI. Wskazanie osób uprawnionych do komunikowania się z wykonawcami

Zamawiający wyznacza następujące osoby do kontaktu z wykonawcami:

1. W zakresie zamówień publicznych – Monika Maksymów, monika.maksymow@um.miastko.pl,, tel. 598570774.
2. W zakresie przedmiotu zamówienia – Marcin Woszczak: : informatyk@um.miastko.pl., tel.598570779.

XXII. Termin związania ofertą

1. Wykonawca jest związany ofertą od dnia upływu terminu składania ofert do **dnia 17.12.2024 r.**
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania oferta określonego w SWZ, zamawiający przed upływem terminu związania oferta 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 oferta, o którym mowa w poz. 2, wymaga złożenia przez wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania oferta.
4. Odmowa wyrażenia zgody, o której mowa w poz. 2, powoduje odrzucenie oferty wykonawcy.

XXIII. Opis sposobu przygotowania oferty

1. Ofertę należy przygotować zgodnie z zasadami określonymi w niniejszym rozdziale.
2. Do przygotowania oferty zaleca się wykorzystanie Formularza Oferty, którego wzór stanowi Załącznik nr 1.do swz. W przypadku, gdy Wykonawca nie korzysta z opracowanego przez Zamawiającego wzoru, w treści oferty należy zamieścić wszystkie informacje wymagane w Formularzu Ofertowym.
3. Oferta musi być sporządzona:
   1) w języku polskim;
   2) w postaci elektronicznej w formacie danych zgodnym z Obwieszczeniem Prezesa Rady Ministrów z dnia 9 listopada 2017 r. w sprawie ogłoszenia tekstu jednolitego rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych" - przy czym Zamawiający zaleca wykorzystanie formatów: .pdf, .doc, .xls, .jpg, (.jpeg) **ze szczególnym wskazaniem na format .pdf;**
   3) podpisana kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione do reprezentowania Wykonawcy.
4. W procesie składania oferty, w tym dokumentów składanych wraz z ofertą na Platformie, kwalifikowany podpis elektroniczny lub podpis zaufany lub podpis osobisty wykonawca może złożyć bezpośrednio na dokumencie, który następnie przesyła do systemu (opcja rekomendowana przez dostawcę Platformy) oraz dodatkowo dla całego pakietu dokumentów w kroku drugim Formularza składania oferty (po kliknięciu w przycisk Przejdź do podsumowania).
5. Podpisy kwalifikowane wykorzystywane przez wykonawców do podpisywania wszelkich plików muszą spełniać „Rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (elDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku".

6. Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi max 10MB, oraz na ograniczenie wielkości plików podpisywanych profilem w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi max. 5MB.
7. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny. Zamawiający wymaga dołączenia odpowiedniej ilości plików, podpisywanych plików z danymi oraz plików XAdES.
8. Informacje dodatkowe – (zalecenia zamawiającego):
   1) ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu, w miarę możliwości, przekonwertowanie plików składających się na ofertę na format .pdf i opatrzenie ich podpisem kwalifikowanym PadES;
   2) pliki w innych formatach niż PDF opatrzyć zewnętrznym podpisem XAdES. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym;
   3) w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju, podpisywanie różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików;
   4) aby wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty;
   5) aby komunikacja z wykonawcami odbywała się tylko na Platformie za pośrednictwem formularza „Wyślij wiadomość do zamawiającego", nie za pośrednictwem adresu e-mail;
   6) jeżeli wykonawca pakuje dokumenty np. w plik ZIP wcześniejsze podpisanie każdego ze skompresowanych plików;
   7) nie wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich podpisem kwalifikowanym, ponieważ może to skutkować naruszeniem integralności plików co równoważne będzie z koniecznością odrzucenia oferty w postępowaniu.
9. Zamawiający, zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020 r. poz. 2452), określa niezbędne wymagania sprzętowo – aplikacyjne umożliwiające pracę na platforma zakupowa.pl:
   1) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s.;
   2) komputer klasy PC lub MAC o następującej konfiguracji:
      a) pamięć min. 2 GB Ram,
      b) procesor Intel IV 2 GHZ lub jego nowsza wersja,
      c) jeden z systemów operacyjnych - MS Windows 7, Mac Os x 104, Linux, lub ich nowsze wersje D
   3) zainstalowana dowolna przeglądarka internetowa, w przypadku Internet Explorer minimalnie wersja 100.;
   4) włączona obsługa JavaScript;
   5) zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf;
   6) platforma zakupowa.pl działa według standardu przyjętego w komunikacji sieciowej – kodowanie UTF8;
   7) oznaczenie czasu odbioru danych przez platformę stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.
10. Sposób zaszyfrowania oferty opisany został w **Instrukcji składania ofert** dostępnej pod adresem: https://drive.google.com/file/d/1Kd1DttbBeiNWt4q4slS4t76lZVKPbkyD/view
11. W godnie z art. 18 ust. 3 ustawy Pzp, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010 i 1649), jeżeli wykonawca, wraz z przekazaniem takich informacji, zastrzegł, że nie mogą być one udostępniane oraz wykazał, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Na Platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.
    Wykonawca wraz z przekazaniem tych informacji zobowiązany jest wykazać spełnienie przesłanek określonych w art. 11 ust. 2 ustawy przywołanej powyżej. Zastrzeżenie przez wykonawcę tajemnicy przedsiębiorstwa bez uzasadnienia, będzie traktowane przez Zamawiającego jako bezskuteczne ze względu na zaniechanie przez Wykonawcę podjęcia niezbędnych działań w celu zachowania poufności objętych klauzulą informacji zgodnie z postanowieniami art. 18 ust. 3 Pzp.

12. Wykonawca, za pośrednictwem platformazakupowa.pl może przed upływem terminu do składania ofert zmienić lub wycofać ofertę. Sposób dokonywania zmiany lub wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcie
13. Każdy z wykonawców może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty zawierającej rozwiązania wariantowe podlegać będzie odrzuceniu.
14. W przypadku przekazywania przez wykonawcę dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku odpowiednio kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
15. Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty wynosi 150 MB natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.
16. Postępowanie prowadzone jest w języku polskim. Oznacza to, że oferta, oświadczenia oraz każdy dokument złożony wraz z ofertą sporządzony w języku obcym winien być złożony wraz z tłumaczeniem na język polski.

XXIV. Sposób oraz termin składania ofert

1. Ofertę wraz z wymaganymi dokumentami należy umieścić na Platformie pod adresem: https://platformazakupowa.pl/um_miastko na stronie dotyczącej odpowiedniego postępowania do dnia **18.11.2024 r., godz.12.**
2. Do oferty należy dołączyć wszystkie wymagane w SWZ dokumenty.
3. Po wypełnieniu Formularza składania oferty i załadowaniu wszystkich wymaganych załączników należy kliknąć przycisk **„Przejdź do podsumowania"**.
4. Oferta składana elektronicznie musi zostać podpisana elektronicznym podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym. W procesie składania oferty za pośrednictwem Platformy, wykonawca powinien złożyć podpis bezpośrednio na dokumentach przesłanych za pośrednictwem Platformy. Zaleca się stosowanie podpisu na każdym załączonym pliku osobno, w szczególności w przypadku wskazanym w art. 63 ust. 2 ustawy Pzp, gdzie zaznaczono, iż oferty oraz oświadczenie, o którym mowa w art. 125 ust. 1 ustawy Pzp sporządza się, pod rygorem nieważności, w formie elektronicznej (opatrzonej kwalifikowanym podpisem elektronicznym) lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.
5. Za datę złożenia oferty przyjmuje się datę jej przekazania w Platformie w drugim kroku składania oferty poprzez kliknięcie przycisku **„Złóż ofertę"** i wyświetlenie się komunikatu, że oferta została zaszyfrowana i złożona.
6. Szczegółowa instrukcja dla wykonawców dotycząca sposobu złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje

XXV. Termin otwarcia ofert

1. Otwarcie ofert nastąpi w dniu **18.11. 2024 r., godz.12.15.**
2. Otwarcie ofert nie jest jawne.
3. Jeżeli otwarcie ofert następuje przy użyciu systemu teleinformatycznego, w przypadku awarii tego systemu, która powoduje brak możliwości otwarcia ofert w terminie określonym przez zamawiającego, otwarcie ofert następuje niezwłocznie po usunięciu awarii.
4. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
5. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
6. Zamawiający, niezwłocznie po otwarciu ofert, udostępni na Platformie w sekcji **„Komunikaty"** na stronie danego 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.

XXVI. Sposób obliczenia ceny

1. Cena oferty musi być podana liczbowo w Formularzu składania oferty sporządzonym według wzoru zawartego w Rozdziale XXXI SWZ.

2. Wykonawca obliczy cenę oferty brutto w tabeli zamieszczonej w Formularzu składania oferty oddzielnie dla każdej części zamówienia na którą składa swoją ofertę, z zastrzeżeniem, że Wykonawca jest zobowiązany do wypełnienia i określenia wartości we wszystkich pozycjach występujących w Formularzu Oferty.
3. Wykonawca w złożonej ofercie musi zaoferować cenę jednoznaczną i ostateczną. Podanie ceny wariantowej wyrażonej jako przedział cenowy lub zawierającej warunki i zastrzeżenia, spowoduje odrzucenie oferty Wykonawcy.
4. Cena oferty musi być wyrażona w złotych polskich (PLN), z dokładnością nie większą niż dwa miejsca po przecinku (zasada zaokrąglania – poniżej 0,005 należy zaokrąglić w dół, powyżej i równe należy zaokrąglić w górę).
5. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).
6. Cena oferty musi obejmować wszelkie koszty związane z wykonaniem przedmiotu zamówienia jakie będzie ponosił Wykonawca, w tym także koszty dostarczenia przedmiotu zamówienia do siedziby zamawiającego, koszty świadczeń gwarancyjnych, podatek VAT, ewentualne upusty i rabaty oraz wykonanie wszystkich innych obowiązków wykonawcy, niezbędnych do zrealizowania przedmiotu zamówienia, zgodnie z umową, załącznikami do niej, oraz postanowieniami SWZ, jak i ewentualne ryzyka wynikające z okoliczności, których nie można było przewidzieć w chwili składania oferty. Nie uwzględnienie powyższego przez Wykonawcę w zaoferowanej przez niego cenie nie będzie stanowić podstawy do ponoszenia przez Zamawiającego jakichkolwiek dodatkowych kosztów w terminie późniejszym.
7. Zgodnie z art. 225 ustawy Pzp, jeżeli została złożona oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą z 11 marca 2004 r. o podatku od towarów i usług, do celów zastosowania kryterium ceny lub kosztu zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć. W takiej sytuacji Wykonawca ma obowiązek:
   1) poinformowania Zamawiającego, że wybór jego oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego,
   2) wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego,
   3) wskazania wartości towaru lub usługi objętych obowiązkiem podatkowym zamawiającego, bez kwoty podatku,
   4) wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą wykonawcy będzie miała zastosowanie. Stosowną informację Wykonawca zobowiązany jest dopisać w Formularzu Oferty. Brak złożenia przez Wykonawcę ww. informacji będzie postrzegany jako brak powstania obowiązku podatkowego u Zamawiającego.
8. Jeżeli Wykonawca ma zamiar zaproponować jakieś rabaty lub upusty cen, powinien je od razu ująć w obliczeniach ceny tak, aby wyliczona cena za realizację zamówienia była ceną całościową. Późniejsze, np. w trakcie otwierania ofert, propozycje obniżek ceny nie będą przyjmowane przez Zamawiającego do wiadomości. Proponowana cena łączna powinna być podana w wysokości ostatecznej tak, aby Zamawiający nie musiał już dokonywać żadnych obliczeń, przeliczeń itp. działań w celu jej określenia. Zamawiający zgodnie z art. 223 ust. 2 ustawy Pzp poprawia omyłki w ofercie.

XXVII. Opis kryteriów oceny ofert, wraz z podaniem wag tych kryteriów i sposobu oceny ofert

1. Kryteria oceny ofert

1.1. Przy wyborze najkorzystniejszej oferty Zamawiający będzie kierował się następującymi kryteriami:
Cena oferty – 60%
Termin realizacji zamówienia - 40%

1.2. Oferty będą oceniane w odniesieniu do najkorzystniejszych warunków przedstawionych przez wykonawców w zakresie wymienionych kryteriów w odniesieniu do poszczególnych części zamówienia zawartych
w ofercie;

1.3. oferta wypełniająca w najwyższym stopniu te kryteria otrzyma maksymalną ilość punktów. Pozostałe oferty otrzymają odpowiednio mniejszą ilość punktów

2. **Sposób oceny ofert** (ocena punktowa):

2.1. **Kryterium „cena oferty" – waga 60%**

Ocena oferty zostanie przeprowadzona na podstawie ceny oferty wskazanej przez Wykonawcę w ofercie przeliczonej na ilość punktów wg wzoru:

$$Pc = \frac{\text{Najniższa cena brutto spośród złożonych (ważnych) ofert (brutto)}}{\text{Cena oferty badanej (brutto)}} \times 100 \times 60\%$$

gdzie:
Pc – ilość punktów uzyskanych przez ofertę badaną.
Badana oferta może uzyskać maksymalnie 60 pkt.

2.2. **Kryterium „termin realizacji zamówienia" – waga 40%**

Kryterium termin realizacji zamówienia punkty będą liczone w następujący sposób:
Punkty w tym kryterium zostaną przyznane na podstawie zaoferowanego przez Wykonawcę w Formularzu ofertowym **(Załącznik nr 2 do swz)** terminu realizacji dostawy. Zamawiający dokona oceny ofert w kryterium „termin realizacji dostawy" zgodnie z poniższą tabelą:

Pt = (Tmax - Tw)/10 x 40

gdzie:
Pt - ilość punktów za termin dostawy (max. 40)
Tw – termin dostawy danego Wykonawcy – w dniach
Tmax – maksymalny termin dostawy – w dniach
Maksymalny termin dostawy wymagany przez Zamawiającego wynosi :
Cz.I- 90 dni.
Cz. II – 30 dni.
Termin dostawy oceniany będzie w zakresie
Cz. I - **od 80 do 90 dni** – (10 dni).
Cz. II – **od 20-30 dni** (10 dni)
Termin dostawy należy podać w Formularzu Ofertowym. W przypadku podania rozbieżnych okresów terminu dostawy przedmiotu zamówienia w innej części oferty lub dokumentach załączonych do oferty Zamawiający za prawidłowy przyjmie termin dostawy podany w Formularzu Ofertowym.
W przypadku zaoferowania terminu dostawy Cz. I - dłuższego niż 90 dni / Cz. II – dłuższego niż 30 dni oferta zostanie odrzucona. W przypadku nie wpisania w Formularzu Ofertowym terminu dostawy Zamawiający uzna, iż Wykonawca oświadcza, że termin dostawy wynosi Cz. I -90 dni/ cz. II – 30 dni.
W przypadku podania terminu krótszego niż Cz. I -80 dni / Cz. II-30 dni Zamawiający przyjmie na potrzeby przyznania punktów w ramach przedmiotowego kryterium termin cz. I 80 dni/ Cz. II-30 dni .

3. Wybór najkorzystniejszej oferty

3.1. Za najkorzystniejszą – w odniesieniu do każdej części zamówienia - zostanie uznana oferta, która będzie przedstawiała najkorzystniejszy bilans ceny i kryterium gwarancji tj. uzyska największą łączną ilość punktów obliczoną wg wzoru:

$$\mathbf{P = Pc + Pt,}$$

gdzie:

P – łączna ilość punktów
Pc – ilość punktów uzyskanych w kryterium „cena oferty"
Pt – ilość punktów uzyskanych w kryterium „termin realizacji zamówienia."

Najkorzystniejsza oferta może maksymalnie uzyskać łącznie 100 pkt za kryteria z uwzględnieniem ich wag.

3.2. Oferty będą oceniane w odniesieniu do najkorzystniejszych warunków przedstawionych przez wykonawców, w zakresie wymienionych kryteriów.
3.3. Oferta wypełniająca w najwyższym stopniu poszczególne kryteria otrzyma maksymalną ilość punktów w danym kryterium.
3.4. Pozostałe oferty otrzymają odpowiednio mniejszą ilość punktów.

3.5. 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.
3.6. Zamawiający wybiera najkorzystniejszą ofertą w terminie związania ofertą określonym w swz.
3.7. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania oferta określonego w swz, zamawiający przed upływem terminu związania oferta zwraca się jednokrotnie do wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.
3.8. Przedłużenie terminu związania oferta, o którym mowa w poz. 3.7., wymaga złożenia przez wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania oferta.
3.9. Odmowa wyrażenia zgody, o której mowa w poz. 3.8., powoduje odrzucenie oferty wykonawcy.
3.10. Zamawiający udzieli zamówienia wykonawcy, który spełni warunki udziału w postępowaniu wynikające z treści swz, Pzp, a jego oferta spośród ofert nie podlegających odrzuceniu została oceniona jako najkorzystniejsza w oparciu o określone w swz kryteria oceny ofert.

XXVIII. 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 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 Nr 10 do SWZ. Umowa zostanie uzupełniona o zapisy wynikające ze złożonej oferty.
5. 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.
6. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (np. na podstawie umowy konsorcjalnej, działalności prowadzonej w formie spółki cywilnej) w przypadku uznania ich oferty za najkorzystniejszą zobowiązani są do przedłożenia zamawiającemu nie później niż w dniu zawarcia umowy:
   1) w przypadku zawiązania konsorcjum - egz. umowy regulującej ich współpracę (konsorcjalnej) jaką zawarli miedzy sobą w celu wspólnej realizacji zamówienia, najpóźniej w dniu wyznaczonym na zawarcie umowy z zamawiającym, przed jej podpisaniem.
      Wymagane jest aby zawarta umowa:
      a) zawierała określenie celu gospodarczego,
      b) wskazywała pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego,
      c) zakazywała wnoszenia zmian w jej treści bez zgody zamawiającego,
      d) stwierdzała, że partnerzy zawartej umowy będą odpowiedzialni solidarnie za całość podjętych zobowiązań w ramach realizacji przedmiotu zamówienia,
      e) była zawarta na czas trwania umowy, powiększony o okres obowiązywania rękojmi i gwarancji,
      f) wykluczała możliwość wypowiedzenia umowy konsorcyjnej przez, któregokolwiek z jego członków do czasu wykonania zamówienia i upływu czasu rękojmi i gwarancji,
      g) była zawarta z notarialnie potwierdzonymi podpisami;
   2) w przypadku Wykonawców prowadzących działalność gospodarczą w formie spółki cywilnej - kopię umowy spółki cywilnej poświadczoną za zgodność z oryginałem przez wspólników spółki.

XXIX. Informacje dotyczące zabezpieczenia należytego wykonania umowy

Zamawiający nie wymaga zabezpieczenia należytego wykonania umowy

XXX. 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 szkodą w wyniku naruszenia przez zamawiającego przepisów 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 Pzp, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargą wnosi się do Sądu Okresowego w Warszawie za pośrednictwem Prezesa Krajowej Izby Odwoławczej .
5. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX „Środki ochrony prawnej" Pzp.

XXXI. Załączniki do SWZ

1. Opis techniczny oferowanego przedmiotu zamówienia- - załącznik nr 1
2. Formularz oferty (wzór) - załącznik nr 2.
3. Wykaz oferowanego sprzętu wraz z szczegółowym opisem technicznym- cz. I -załącznik 2a.
4. Wykaz oferowanego oprogramowania wraz z szczegółowym opisem technicznym- cz.II – załącznik 2b.
5. Oświadczenie wykonawcy o niepodleganiu wykluczeniu - załącznik nr 3.
6. Oświadczenie wykonawcy o spełnianiu warunków udziału - załącznik nr 4.
7. Oświadczenie wykonawcy o braku przynależności do tej samej grupy kapitałowej - załącznik nr 5.
8. Oświadczenie podmiotu udostępniającego zasoby wykonawca o braku podstaw wykluczenia oraz spełnianiu warunków udziału - załącznik nr 6.
9. Zobowiązanie podmiotu udostępniającego zasoby, do ich oddania wykonawcy - załącznik nr 7.
10. Wykaz dostaw - załącznik nr 8.
11. Wykaz osób załącznik nr 9.
12. Wzór umowy - załącznik nr 10.
13. Klauzula informacyjna dotycząca przetwarzania danych osobowych „RODO" - załącznik nr 11.

ZAŁĄCZNIK NR 1 DO SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

na dostawę i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko

Miastko, 2024

Spis treści

Rozdział I. Założenia początkowe oraz wymagania ogólne

I.1 Wprowadzenie i cel projektu

Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko realizowane jest w ramach programu „Cyberbezpieczny Samorząd", którego celem jest zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego (JST) poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych.

I.2 Akty prawne

Dostarczane w ramach prowadzonego postępowania rozwiązania muszą być zgodne z obowiązującymi przepisami prawa zarówno polskiego, jak i europejskiego. Ważne jest, aby oprogramowanie umożliwiało bezpieczne gromadzenie, przetwarzanie i analizowanie danych w obszarach objętych wdrożeniem.

I.3 Ogólny opis przedmiotu zamówienia:

Przedmiot zamówienia podzielony jest na dwie części:

1) **Część nr 1** obejmuje rozbudowę infrastruktury informatycznej urzędu opartą na dostawie sprzętu wraz z instalacją, montażem i przeniesieniem danych z obecnej sieci informatycznej oraz wdrożenie oprogramowania do zarządzania siecią IT wraz z konfiguracją sieci VLAN. Wykonawca jest zobowiązany do sporządzenia dokumentacji z przeprowadzonego wdrożenia oraz przeprowadzenia szkoleń specjalistycznych z zastosowanych rozwiązań. **Szczegółowe opisy minimalnych parametrów technicznych urządzeń, oprogramowania i szkoleń w ramach zadania dla części nr 1 zostały opisane w rozdziale II:**

Poz. OPZ	**Opis**	**Ilość sztuk/kpl**
Rozdział	**Rodzaj zamawianego asortymentu**	
II.1.1	Serwer I - Dostawa, instalacja i wdrożenie serwerów w celu utworzenia klastra pracy awaryjnej urzędu. Konfiguracja klastra	3 szt.
II.1.2	Serwer II - Dostawa serwera	1 szt.
II.1.3	Oprogramowanie i licencje do serwerów	Zgodnie z opisem
II.1.4	Macierz - Dostawa, instalacja, konfiguracja macierzy z klastrem pracy awaryjnej, Przeniesienie danych z dotychczasowych nośników.	1 szt.
II.1.5	Dostawa i wdrożenie oprogramowania do wykonywania kopii zapasowych wraz z usługą chmurową	1 szt.
II.1.6	Wdrożenie oprogramowania do zarządzania infrastrukturą IT na 80 licencji	1 szt.
II.1.7	Wdrożenie usług domeny do zarzadzania siecią i zasobami komputerowymi	1 szt.
II.1.8	Przełącznik dystrybucyjny L3	1 szt.
II.1.9	Przełączniki sieciowe - Dostawa i wdrożenie zarządzalnych przełączników sieciowych do utworzenia rdzenia sieci LAN	6 szt.
II.1.10	Dostawa, instalacja oraz podłączenie zasilacza awaryjnego UPS z kartą SNMP	1 szt.
II.1.11	Dostawa wraz z montażem i uruchomieniem dysków 12TB przeznaczonych do wykonywania kopii zapasowych	5 szt.
II.1.12	Szkolenie ASI tworzenie i administracja sieci VLAN	1 szt.
II.1.13	Szkolenie ASI tworzenie i administracja serwerami Windows	1 szt.
II.1.14	Szkolenie ASI z domeny do zarzadzania siecią i zasobami komputerowymi	1 szt.
II.1.15	Szkolenie ASI Budowa klastra Hyper-V	1 szt.
II.1.16	Szkolenie z oprogramowania do zarządzania infrastrukturą IT	1 szt.

Tabela nr 1 – Spis urządzeń dla części nr 1

2) **Część nr 2** obejmuje dostawę oprogramowania do monitorowania infrastrukturą sieci informatycznej i urządzeń dla jednostki podległej oraz dostawę usług chmurowych w ramach zabezpieczenia poczty i

stron internetowych Gminy. **Szczegółowe opisy minimalnych parametrów technicznych urządzeń, oprogramowania i szkoleń w ramach zadania dla części nr. 2 zostały opisane w rozdziale II**:

Poz. OPZ	Opis	Ilość sztuk/kpl
Rozdział	**Rodzaj zamawianego asortymentu**	
II.2.1	Oprogramowanie do zarządzania infrastrukturą IT na 31 licencji dla MOPS	1 szt.
II.2.2	Usługa zabezpieczenia poczty	1 szt.
II.2.3	Usługa zabezpieczenia serwisu www na 24 miesiące	1 szt.

Tabela nr 2 – Spis urządzeń dla części nr 2

2. Przedmiot zamówienia musi być dostarczany, wdrożony i zainstalowany w całości do siedziby Zamawiającego.
3. **Zamawiający wymaga załączenia do Formularza ofertowego wykazu oferowanego sprzętu wraz ze szczegółowym opisem technicznym (dla każdej z części na którą jest składana oferta) - Znajdującego się w Załączniku nr 2a - Wykaz oferowanego sprzętu wraz z szczegółowym opisem technicznym/ Załącznik nr 2 b Wykaz oferowanego oprogramowania wraz z szczegółowym opisem technicznym** - w taki sposób aby Zamawiający mógł jednoznacznie określić szczególne cechy produktu oraz wymagane prawem certyfikaty, deklaracje zgodności CE, instrukcje obsługi sprzętu, dokumenty gwarancyjne, celem sprawdzenia zgodności oferowanego produktu.
4. Jeżeli w opisie przedmiotu zamówienia wskazano jakikolwiek znak towarowy, patent lub pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę – należy przyjąć, że Zamawiający podał taki opis w celu określenia **minimalnych parametrów**, jakim muszą odpowiadać produkty, aby spełnić wymagania stawiane przez Zamawiającego i stanowią one wyłącznie wzorzec jakościowy przedmiotu zamówienia, a nie wskazanie na konkretny wyrób danego producenta. Zgodnie z art. 99 ust. 5 ustawy Prawo zamówień publicznych. Zamawiający dopuszcza możliwość złożenia oferty równoważnej, jednak pod warunkiem, że zaproponowany przez Wykonawcę produkt równoważny będzie spełniał minimum wymogów tej samej klasy jakiej oczekuje Zamawiający, tzn. będzie odpowiadał wymaganiom opisanym przez Zamawiającego w SWZ. Asortyment zaproponowany jako równoważny nie może odbiegać jakością, standardem, parametrami technicznymi od założonych przez Zamawiającego. Za asortyment równoważny Zamawiający uzna ten, który posiada te same lub lepsze od opisanych w SWZ parametry techniczne i jakościowe, a jego zastosowanie w żaden sposób nie wpłynie na prawidłowe funkcjonowanie infrastruktury informatycznej Zamawiającego. Wykonawca, który powołuje się na rozwiązania równoważne jest zobowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. Ciężar dowodowy w zakresie udowodnienia równoważności zaoferowanych rozwiązań z rozwiązaniami opisanymi poprzez wskazanie przykładowego znaku towarowego, patentu lub pochodzenia, spoczywa na Wykonawcy, składającym ofertę równoważną. Wykonawcy powinni oznaczyć, której części oraz którego punktu tabeli załącznika nr 2a do SWZ - Wykaz oferowanego sprzętu wraz z szczegółowym opisem technicznym/2b Wykaz oferowanego oprogramowania wraz z szczegółowym opisem technicznym dokumenty dotyczą. Jeżeli w prospektach brak opisu danego wymogu, dopuszcza się załączenie do oferty innych dokumentów, w których Zamawiający będzie w stanie zweryfikować zgodność opisu danego wymogu lub oświadczenie producenta. Zamawiający dopuszcza także oświadczenie własne wykonawcy w przypadku gdy dany parametr nie można potwierdzić w inny sposób.
5. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca przeprowadzi zgodnie z zapisami niniejszego OPZ w uzgodnieniu z Zamawiającym, zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów informatycznych oraz najlepszymi praktykami w ich realizacji.
6. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, zapisami OPZ oraz Umowy.
7. Wykonawca musi dostarczyć wszelkie urządzenia i elementy, które są niezbędne do prawidłowego funkcjonowania całości. W przypadku, gdy w trakcie realizacji Przedmiotu Zamówienia okaże się, że brakuje jakiegokolwiek urządzenia, elementu i/lub licencji, którego brak spowoduje nieprawidłowe funkcjonowanie całości Przedmiotu Zamówienia, Wykonawca dostarczy je na własny koszt.
8. Wszelkie dostarczane urządzenia:
   - Muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta.
   - Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych.

- Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.
- Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.
- Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
- Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta.
- Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.

I.4 Termin realizacji Przedmiotu Zamówienia

Termin realizacji Przedmiotu zamówienia wynosi :

1) Cz. I - nie więcej niż **90 dni** kalendarzowych od dnia zawarcia Umowy.
2) Cz.II - nie więcej niż **30 dni** kalendarzowych od dnia zawarcia Umowy.

I.5 Założenia podstawowe:

1. Przedmiot Zamówienia będzie realizowany w oparciu o zdefiniowany uprzednio przez Wykonawcę i zaakceptowany Harmonogram wdrożenia, który powinien być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia.
2. Wykonawca w Harmonogramie wdrożenia musi uwzględnić w szczególności podział na zadania takie jak projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.
3. Wykonawca umożliwi Zamawiającemu udział we wszystkich pracach realizowanych przez Wykonawcę w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie projektowania, dostawach, instalacji/budowie, konfiguracji, wdrożeniu i testowaniu).
4. Wykonawca zobowiązany jest przeprowadzić dostawy Przedmiotu Zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.
5. W przypadku dostarczania infrastruktury serwerowej musi być ona oznakowana w taki sposób, aby możliwa była identyfikacja systemowa zarówno produktu jak i producenta, pochodzić z oficjalnych kanałów dystrybucji producentów i dostarczona w oryginalnych opakowaniach fabrycznych.
6. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie Przedmiotu Zamówienia.
7. Wykonawca jest zobligowany do powołania i przedstawienia przed przystąpieniem do pracy zespołu wdrożeniowego, w którego skład będzie wchodził kierownik zespołu.
8. Wykonawca zorganizuje prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania pracy Zamawiającego.
9. Wykonawca musi uwzględnić, że wszystkie prace wykonywane będą w użytkowanych obiektach przy dużym ruchu pracowników i interesantów urzędu.
10. Wykonawca zobowiązany jest opracować na podstawie SWZ oraz OPZ szczegółowy harmonogram wdrożenia. Harmonogram należy przedstawić Zamawiającemu w terminie do 14 dni od podpisania Umowy.
11. Harmonogram planowanych prac wdrożeniowych uwzględniać będzie m.in. dostawę sprzętu, instalację i wdrożenie oprogramowania, przeniesienie danych z obecnej infrastruktury gminy oraz szkolenia dla administratorów.
12. Harmonogram podlega zatwierdzeniu przez Zamawiającego.

I.6 Dokumentacja Powykonawcza

1. Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację użytkową, techniczną i eksploatacyjną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej bądź papierowej.
2. W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań.
3. W szczególności dokumentacja ta powinna zawierać następujące elementy:
    a. Schemat infrastruktury i architekturę rozwiązania wraz z opisem.
    b. Zasady licencjonowania dostarczonych elementów.
    c. Konfigurację sprzętową i logiczną elementów infrastruktury dla wdrożonych systemów.
    d. Procedury uruchamiania, zatrzymywania wdrożonych systemów oraz elementów infrastruktury.

e. Procedury konfiguracji kont w dostarczonych systemach.
f. Procedury awaryjne umożliwiające dostęp do infrastruktury w przypadku awarii.
g. Procedury wykonywania odtworzenia wdrożonych systemów z kopii zapasowej.
h. Procedury opisujące standardowe działania administracyjne.
i. Procedury odzyskania wdrożonych systemów po awarii.
j. Wytyczne (dobre praktyki) dla administratorów.
k. Spis dokumentacji zewnętrznej do której odwołuje się Dokumentacja Powykonawcza.

I.7 Odbiór Dokumentacji/Końcowy

1. Odbiór końcowy Przedmiotu Zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy oraz dostarczenia wymaganej zamówieniem Dokumentacji.
2. Odbiory będą odbywać się zgodnie z zapisami w Umowie stanowiącym Załącznik nr 10 do SWZ.

I.8 Testy

1. W ramach postępowania zostaną przeprowadzone wszystkie testy opisane w dokumentacji. Celem testów jest weryfikacja przez Zamawiającego czy wszystkie prace wykonane w trakcie realizacji Przedmiotu Zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale Zamawiającego jak i wskazanych przez Zamawiającego osób lub podmiotów zewnętrznych.
2. Zamawiający w końcowej fazie wdrożenia oczekuje realizacji przez Wykonawcę testów bezpieczeństwa.
3. W przypadku zidentyfikowania błędów lub wad Wykonawca jest zobowiązany do ich poprawy przed odbiorem Końcowym Przedmiotu Zamówienia.
4. Zamawiający wymaga, aby Wykonawca przeprowadził testy odbiorcze co najmniej z zakresu:
   a) Uruchamianie i zatrzymywanie wdrożonych systemów
   b) Weryfikacja wdrożonych systemów zgodnie ze scenariuszami opisanymi w dokumentacji.
   c) Weryfikacja poprawności działania procedur.
   d) Symulację awarii wdrożonych systemów.

I.9 Dodatkowe zobowiązania Wykonawcy

1. Wykonawca zobowiązany jest wykonać Przedmiot Zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.
2. Wykonawca zobowiązany jest wykonać w całości Przedmiot Zamówienia w zakresie określonym w Umowie będącej Załącznikiem nr 10 do SWZ.
3. Wykonawca zobowiązany jest do uzgodnienia z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz zachowania ciągłości współpracy z Zamawiającym na każdym etapie realizacji.
4. Wykonawca zobowiązany jest do stosowania się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.
5. Wykonawca zobowiązany jest do udzielania na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
6. Wykonawca zobowiązany jest do współdziałania z osobami wskazanymi przez Zamawiającego.

Rozdział II. Szczegółowy opis przedmiotu zamówienia

II.1 Minimalne parametry wdrożenia dla Części nr 1

1. Przedmiotem zamówienia dla części nr 1 jest przeprowadzenie kompleksowej rozbudowy infrastruktury informatycznej Zamawiającego na podstawie dostaw, instalacji i wdrożenia rozwiązań zaplanowanych w ramach programu „Cyberbezpieczny samorząd"
2. Minimalne wymagane parametry techniczne wszystkich urządzeń zostały opisane w rozdziale II zgodnie z tabelą nr 1 – Spis urządzeń dla części nr 1.
3. W ramach tego zadania Wykonawca zobowiązany jest do dostarczenia wszystkich niezbędnych elementów wymaganych do instalacji, podłączenia i konfiguracji urządzeń informatycznych tj. kable połączeniowe, łączniki, elementy mocujące, oraz wszystkie uznane przez Wykonawcę elementy uznane za niezbędne do prawidłowego uruchomienia i zamontowania infrastruktury będącej przedmiotem zamówienia. Zamawiający wymaga aby wszelkie niezbędne elementy były wkalkulowane w koszt oferty Wykonawcy.
4. Po przeprowadzeniu wdrożenia Wykonawca przekaże Zamawiającemu wszystkie niezbędne hasła dostępowe, dokumentację do wszystkich oferowanych urządzeń i zainstalowanego oprogramowania wraz z dokumentami potwierdzającymi legalność licencji nabytych dla Zamawiającego. Wykonawca

przeprowadzi również instruktaż z przeprowadzonego wdrożenia wskazanym przez Zamawiającego administratorom.

5. W ramach rozbudowy serwerowni Wykonawca zainstaluje dostarczony sprzęt i dokona konfiguracji urządzeń zgodnie z poniższymi założeniami:
   1) Wykonawca zapozna się z konfiguracją starych przełączników sieciowych w taki sposób aby po ich wymianie na nowe przełączniki skonfigurować je dokładnie tak samo. Następnie wymontuje z szafy stare przełączniki, zainstaluje nowe przełączniki w miejsce starych, przeprowadzi konfigurację oraz uporządkuje okablowanie.
   2) Wykonawca zainstaluje światłowodowy przełącznik dystrybucyjny zwany dalej przełącznikiem L3,
   3) Każdy z przełączników dostępowych za pomocą dedykowanych portów Uplink 10G lub szybszych powinien zostać wpięty do przełącznika L3 za pomocą odpowiednich wkładek oraz pathcordów światłowodowych.
   4) Wykonawca zainstaluje w szafie macierz oraz serwery w miejscu wskazanym przez wykonawcę.
   5) Połączenia serwerów i macierzy powinny być realizowane z przełącznikiem L3 za pomocą portów 25Gb/s, każdy z serwerów powinien być połączony dwoma portami 25Gb/s. Macierz powinna zostać wpięta do przełącznika L3 4 portami 25Gb/s po 2 porty na każdy z silników.
   6) Jeden z przełączników dostępowych powinien zostać przeznaczony na przełącznik do obsługi sieci zarządzania, do tego przełącznika powinny zostać wpięte wszystkie urządzenia posiadające porty zarządzania.
   7) Porty zarządzania macierzy z obu silników powinny zostać wpięte do przełącznika zarządzania. Następnie w serwerach porty zdalnego zarządzania serwerem oraz porty karty sieciowej przeznaczone do zarządzania serwerem powinny zostać wpięte do przełącznika zarządzania.
   8) Wszystkie przełączniki sieciowe, serwery, macierz i punkty dostępowe powinny korzystać z logowania jednokrotnego (Single Sign-On), tak aby za pomocą usługi katalogowej, osoby dostające się do urządzeń korzystały ze swoich kont w domenie. Zauważyć należy, że o ile urządzenie na to pozwala to powinno ono zostać tak skonfigurowane, aby w razie braku dostępności usługi katalogowej można było skorzystać ze statycznego hasła ratunkowego.
   9) Obecne w serwerach karty SFP28 które posłużą do podłączenia macierzy z serwerami powinny zostać wyposażone w odpowiednie wkładki SFP28 o prędkości 25Gb/s, a połączenie serwerów z przełącznikiem L3 powinno zostać zrealizowane za pomocą kabli światłowodowych (pathcord).
   10) Każdy z serwerów będzie podłączony dwoma kablami do przełącznika L3, aby zapewnić nadmiarowość.
   11) Do przełącznika zarządzania powinny zostać podłączone inne urządzenia znajdujące się w serwerowni to jest:
      a. Przełączniki sieciowe zarówno te dostarczane w przedmiotowym postępowaniu jak i te które już obecnie znajdują się w serwerowni.
      b. Interfejsy LAN zasilaczy awaryjnych.
      c. Interfejsy zdalnego zarządzania pozostałych serwerów.
   12) Wszystkie urządzenia podłączone do przełącznika zarządzania powinny zostać odpowiednio skonfigurowane aby możliwy był dostęp do tych urządzeń z oprogramowania LMS (Lan Management System), adresację IP oraz numerację VLAN wykonawca otrzyma przed rozpoczęciem prac.
   13) Na serwerach zainstalować należy system operacyjny. System operacyjny powinien obsługiwać możliwość administracji systemem z poziomu samego serwera, czyli w taki sposób aby serwerowy system operacyjny umożliwiał uruchamianie wymaganych aplikacji bezpośrednio na konsoli serwera, administracja serwerem powinna odbywać się za pomocą interfejsu graficznego wykorzystującemu okna.
   14) Serwery powinny posiadać odpowiednio skonfigurowaną sieć. Adresacja sieci powinna być spójna i logiczna. Na serwerach należy skonfigurować sieć w taki sposób aby serwery za pomocą portów SFP28 miały ze sobą wzajemną łączność, żeby znajdowały się w jednej domenie rozgłoszeniowej wraz z portami usługowymi macierzy.
   15) Serwery powinny korzystać z technologii łączności NvmeOverRocev2, tak aby połączenie z macierzą korzystało z wydajności jaką ofertuje ten standard komunikacji.
   16) Serwery należy skonfigurować tak aby tworzyły jeden klaster pracy awaryjnej, chodzi o to aby serwery dysponowały wspólną przestrzenią dyskową, żeby przestrzeń ta mogła być dynamicznie przepinana do poszczególnych serwerów klastra. Obecne na klastrze maszyny wirtualne muszą umożliwiać ich

przenoszenie pomiędzy serwerami klastra bez konieczności wyłączania maszyn wirtualnych (migracja na żywo), migracja maszyn powinna odbywać się z wykorzystaniem szybkich 25GB/s interfejsów. Klaster powinien umożliwiać przełączanie dowolnego z serwerów w tryb serwisowy i pozwalać na odłączenie serwera od zasilania bez ryzyka niestabilności czy niedostępności jakiejkolwiek z maszyn wirtualnych. W razie wystąpienia awarii jednego z serwerów klaster również powinien samoczynnie przywrócić do działania maszyny, które w danym momencie znajdowały się na serwerze, który został wyłączony z użycia w wyniku awarii

17) Wymagania funkcjonalne klastra pracy awaryjnej:

a. Obsługa wirtualizacji przy użyciu roli Hyper-V w systemie Windows Server 2022, umożliwiająca tworzenie, zarządzanie oraz migrację maszyn wirtualnych.
b. Implementacja klastra pracy awaryjnej (Failover Cluster) zapewniającego wysoką dostępność usług oraz automatyczne przenoszenie maszyn wirtualnych pomiędzy węzłami w przypadku awarii.
c. Wsparcie dla funkcji replikacji Hyper-V (Hyper-V Replica) w celu zapewnienia dodatkowego poziomu zabezpieczenia danych.
d. Wsparcie dla Live Migration (migracja na żywo) oraz Storage Migration bez przestojów usług.
e. Możliwość centralnego zarządzania zasobami klastra i maszynami wirtualnymi z poziomu narzędzia Windows Admin Center lub równoważnego.
f. Obsługa skalowania klastra do co najmniej 16 węzłów i wsparcie dla pamięci współdzielonej (Shared Storage).
g. Zintegrowane mechanizmy monitorowania i powiadamiania o stanie klastra oraz maszyn wirtualnych.
h. Wsparcie dla zaawansowanych mechanizmów ochrony danych, takich jak Windows Server Backup oraz integracja z zewnętrznymi rozwiązaniami backupowymi.

18) Wykonawca zmigruje obecne fizyczne środowisko serwerów fizycznych (Bare Metal) i przekształci – przekonwertuje maszyny fizyczne do maszyn wirtualnych z zachowaniem obecnych ustawień oraz danych znajdujących się na tych serwerach. Migracja taka powinna odbyć się w ustalonych oknach serwisowych aby nie destabilizować pracy urzędu.

Lista serwerów do migracji

Urządzenie	**System operacyjny**	**Pełniona funkcja**
Dell R330	Windows Server	Serwer baz danych MsSQL, repozytorium plików
Dell R250	Debian Linux	Serwer www
Dell R250	Debian Linux	Centrala telefoniczna VoIP
Dell R250	Debian Linux	Serwer poczty
Dell R460	Debian Linux	Serwer baz danych MySQL
Dell R460	Debian Linux	Serwer baz danych PostgreSQL
Dell R460	Debian Linux	Serwer systemów dziedzinowych
Dell R460	Debian Linux	Serwer Elektronicznego Obiegu Dokumentów
Dell R460	Debian Linux	Serwer Systemów Rejestrów Państwowych
Dell R460	Debian Linux	Serwer plików samba
Dell R460	Debian Linux	Serwer Traffic
Dell R460	Debian Linux	Serwer Elektronicznego Zarządzania Dokumentacją

19) Oprogramowanie do kopii zapasowych**:** System backup wdrożony zostanie w taki sposób, aby był zgodny z zasadą 3-2-1. Jest to strategia tworzenia kopii zapasowych danych zaprojektowana w celu zapewnienia możliwości szybkiego odzyskania i przywrócenia danych w przypadku incydentu utraty danych. W szczególności ta strategia tworzenia kopii zapasowych musi zapewniać posiadanie trzech niezależnych kopii danych.

a. Wykonawca dostarczy, przeprowadzi instalację oraz konfigurację oprogramowania do tworzenia kopii zapasowych i odzyskiwania danych dla środowisk wirtualnych, chmurowych oraz fizycznych serwerów, spełniające parametry minimalne zgodnie z opisem technicznym.
b. Wykonawca skonfiguruje oprogramowanie kopii zapasowych w taki sposób aby podstawowa kopia zapasowa robiła się raz dziennie w godzinach wieczornych. Kopia różnicowa baz danych i innych kluczowych zbiorów powinna się wykonywać raz na godzinę. Archiwizacja powinna być wykonywana na dedykowane serwery NAS posiadane już przez Zamawiającego. Trzecia kopia zostanie wyniesiona do usługi kopii odmiejscowionej zaoferowanej przez Wykonawcę zgodnie z opisem minimalnych

parametrów technicznych . Archiwizacji powinny podlegać wszystkie serwery wirtualne pracujące na klastrze pracy awaryjnej oraz dane znajdujące się na macierzy.

c. Wymagania funkcjonalne oprogramowania:
   - Wsparcie dla środowisk wirtualnych opartych o VMware, Hyper-V oraz Nutanix.
   - Możliwość tworzenia kopii zapasowych maszyn wirtualnych oraz ich replikacji.
   - Możliwość przywracania pojedynczych plików, obiektów aplikacji oraz całych maszyn wirtualnych.
   - Wsparcie dla deduplikacji i kompresji danych w celu optymalizacji przestrzeni dyskowej.
   - Obsługa chmury publicznej do przechowywania kopii zapasowych (np. AWS, Azure).
   - Możliwość automatyzacji procesów tworzenia kopii zapasowych oraz zarządzania nimi.
   - Szyfrowanie danych podczas przesyłania i w stanie spoczynku.
   - Wsparcie dla rozbudowanych raportów oraz monitorowania procesów tworzenia i przywracania kopii zapasowych.
   - Intuicyjny interfejs użytkownika oraz wsparcie dla centralnego zarządzania backupami w rozproszonych lokalizacjach.
   - Oprogramowanie musi być kompatybilne z infrastrukturą Zamawiającego, w tym z istniejącymi środowiskami wirtualizacji oraz pamięci masowej.
   - Możliwość uruchomienia oprogramowania na systemach operacyjnych z rodziny Linux i Windows.
   - Obsługa protokołów komunikacyjnych dla zdalnego zarządzania oraz monitorowania zadań backupowych.
   - Wsparcie dla integracji z systemami monitorowania IT w celu uzyskiwania powiadomień o statusie zadań.
   - Oprogramowanie musi być dostarczone wraz z licencją na co najmniej 12 miesięcy wsparcia technicznego oraz aktualizacji oprogramowania.
   - Wsparcie techniczne musi obejmować dostęp do pomocy technicznej w formie telefonicznej i e-mailowej w godzinach roboczych.
   - Licencja musi obejmować możliwość ochrony minimalnie 10 maszyn wirtualnych z opcją rozbudowy licencji w przyszłości.

20) Wykonawca dostarczy, zainstaluje oraz skonfiguruje system monitorowania infrastruktury IT, o parametrach minimalnych spełniających wymagania techniczne.
Wymagania funkcjonalne oprogramowania:

a. Monitorowanie sieci: Oprogramowanie musi umożliwiać monitorowanie urządzeń sieciowych (routerów, przełączników, serwerów, urządzeń IoT itp.) z wykorzystaniem protokołu SNMP, ICMP, oraz innych powszechnie stosowanych protokołów monitorowania.
b. Automatyczne wykrywanie urządzeń: Oprogramowanie powinno wspierać automatyczne wykrywanie urządzeń sieciowych w sieci i dodawanie ich do monitorowania.
c. Obsługa wielu producentów: System musi wspierać monitorowanie urządzeń od różnych dostawców, takich jak Cisco, Juniper, Ubiquiti, HP, MikroTik, Dell, Huawei i innych, które posiada w swojej strukturze sieci Zamawiający.
d. Monitorowanie zasobów: Oprogramowanie musi zapewniać monitorowanie zasobów systemowych (procesor, pamięć RAM, przestrzeń dyskowa, interfejsy sieciowe, itp.) dla urządzeń sieciowych i serwerów.
e. Alertowanie i powiadamianie: System musi posiadać zaawansowane funkcje alertowania i powiadamiania o przekroczeniu zdefiniowanych progów dla monitorowanych parametrów, z możliwością wysyłania powiadomień e-mail lub przez inne kanały komunikacyjne (np. SMS, webhook).
f. Raportowanie i wykresy: System powinien umożliwiać generowanie raportów oraz tworzenie wykresów historycznych, przedstawiających zmiany w monitorowanych zasobach.
g. Integracja z zewnętrznymi systemami: Oprogramowanie powinno posiadać API umożliwiające integrację z innymi systemami monitorowania, zarządzania i automatyzacji.
h. Dostęp przez przeglądarkę internetową: System powinien być dostępny poprzez interfejs webowy, umożliwiający zarządzanie oraz przeglądanie wyników monitoringu z poziomu przeglądarki.

i. Skalowalność: Oprogramowanie powinno wspierać monitorowanie zarówno małych, jak i dużych sieci (co najmniej 1000 urządzeń).
j. Bezpieczeństwo: System powinien zapewniać odpowiednie mechanizmy autoryzacji dostępu (np. logowanie z użyciem LDAP, RADIUS lub innego systemu zarządzania użytkownikami) oraz szyfrowanie transmisji danych.
k. System powinien posiadać funkcjonalność syslog, aby można było przekierować komunikaty z urządzeń sieciowych za pomocą tego protokołu.
l. Wymagania techniczne:
    - Możliwość instalacji oprogramowania na systemach operacyjnych z rodziny Linux (preferowane) oraz Windows
    - Obsługa baz danych MySQL lub MariaDB.
    - Możliwość uruchomienia oprogramowania w środowisku wirtualnym lub fizycznym.
    - Wsparcie dla protokołów SNMP (v1, v2c, v3), ICMP, IPv4, IPv6.
m. Licencjonowanie i wsparcie:
    - Wykonawca musi zapewnić co najmniej 24 miesiące wsparcia technicznego w zakresie instalacji, konfiguracji oraz rozwiązywania problemów.
    - Wykonawca zainstaluje system NMS oraz doda do tego systemu wszystkie urządzenia sieciowe znajdujące się w serwerowni i na terenie urzędu tj.: Przełączniki sieciowe zarówno te dostarczane w postępowaniu jak i te które już obecnie znajdują się w serwerowni. (5 szt.); Zasilacze awaryjne (2 szt.); Pozostałe serwery fizyczne (8 szt.); Drukarki sieciowe znajdujące się na terenie urzędu 16 szt. ; Urządzenia NAS – 2 szt.; Macierz; Punkty dostępowe WiFi;
n. Dodatkowe wymagania: Szkolenie dla personelu Zamawiającego w zakresie obsługi oraz administracji systemu monitorowania.
o. Dokumentacja powdrożeniowa, zawierająca opis architektury systemu oraz instrukcję użytkowania.

21) Wykonawca zaprojektuje, dostarczy, zainstaluje, skonfiguruje i wdroży usługę katalogową w środowisku serwerowym w celu centralnego zarządzania użytkownikami, zasobami sieciowymi i politykami bezpieczeństwa w organizacji w zakresie prac obejmującym minimum:

a. Analiza przedwdrożeniowa: Przeprowadzenie analizy istniejącej infrastruktury IT oraz wymagań Zamawiającego oraz audyt sieci oraz serwerów pod kątem zgodności z wymaganiami dla wdrożenia usługi katalogowej.
b. Przygotowanie środowiska: Przygotowanie serwerów katalogowych oraz konfiguracja wymaganych ról (np. systemu nazw domenowych DNS oraz systemu dynamicznego przydzielania adresów IP) oraz konfigurację redundancji serwerów katalogowych w celu zapewnienia wysokiej dostępności (co najmniej 2 serwery katalogowe w tym jeden fizyczny).
c. Wdrożenie usługi katalogowej:
    - Instalacja i konfiguracja usługi katalogowej.
    - Utworzenie nowej struktury katalogowej lub dołączenie do istniejącej struktury katalogowej.
    - Definiowanie jednostek organizacyjnych (OU) oraz struktury grup użytkowników i zasobów.
    - Konfiguracja polityk bezpieczeństwa oraz uprawnień dostępu do zasobów sieciowych.
    - Wdrożenie i konfiguracja mechanizmów logowania jednokrotnego (Single Sign-On) oraz integracja z innymi usługami w środowisku organizacji.
d. Testy wdrożeniowe:
    - Przeprowadzenie testów poprawności działania usługi katalogowej, w tym testy logowania użytkowników, przydzielania zasobów oraz działania polityk bezpieczeństwa.
    - Testowanie redundancji i mechanizmów wysokiej dostępności.
    - Zapewnienie bezpiecznego przeniesienia danych z minimalnym przestojem operacyjnym.
    - Przyłączenie komputerów do usługi katalogowej w taki sposób aby użytkownicy zachowali obecnie posiadane profile i ustawienia swoich komputerów biurkowych – chodzi o to aby nie zachodziła konieczność ponownej konfiguracji programów i usług.
e. Szkolenie personelu: Przeprowadzenie szkolenia dla administratorów i użytkowników w zakresie zarządzania oraz korzystania z tej konkretnej usługi katalogowej.

22) W ramach prac wdrożeniowych Wykonawca zainstaluje w serwerowni kontroler umożliwiający monitorowanie wszystkich funkcji wydajności struktury sieci informatycznej zainstalowany w serwerowni Zamawiającego. Kontroler powinien spełniać poniższe parametry techniczne:

Ekran	- Matryca dotykowa min. 13", max 14" błyszcząca z podświetleniem LED, zalecana rozdzielczość min. 2880 x 1920; - Częstotliwość odświeżania: min 120 Hz;
Płyta główna	Wyposażona przez producenta w dedykowany chipset dla oferowanego procesora. Zaprojektowana na zlecenie producenta, oznaczona trwale na etapie produkcji nazwą lub logiem producenta oferowanego komputera; - Wbudowana karta sieciowa WiFi min.6 - Wbudowany moduł bluetooth min. 5.1 - Wbudowany min. 1x: Akcelerometr Magnetometr Żyroskop
Procesor	- Procesor dla urządzeń mobilnych - Wydajność obliczeniowa: procesor powinien osiągać w teście benchmark, według wyników opublikowanych na stronie www co najmniej wynik 9790 punktów. Wynik dostępny na stronie: http://www.cpubenchmark.net.
Pamięć RAM	Min. 16 GB typu LPDDR4x
Dysk twardy	Min. 256 GB klasy SSD.
Karta graficzna	Zintegrowana
Multimedia	- Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition Audio - Wbudowane głośniki - Przednia kamera min. 5.0MP - Tylna kamera min. 10.0 Mpix
Obudowa	Aluminiowa z rozkładaną podstawką
Porty/złącza	- USB Typu-C (z Thunderbolt™ 4) - 2 szt - Złącze stacji dokującej - 1 szt
Napęd optyczny	Brak
Zasilanie	- Bateria zapewniająca pracę po naładowaniu na min. 10 godzin pracy, - Zasilacz zewnętrzny dedykowany.
System operacyjny	Windows 10 Pro lub Windows 11 Pro lub równoważny
Oprogramowanie dodatkowe	Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci; Partycja recovery (opcja przywrócenia systemu z dysku).
Bezpieczeństwo	Moduł TPM lub równoważny

Minimalne wymagania techniczne dla oferowanych urządzeń:

Dostawa, instalacja i wdrożenie klastra pracy awaryjnej urzędu składającego się z 3 serwerów wraz z systemem operacyjnym.

1. W celu poprawy i zwiększenia efektywności sieci informatycznej Zamawiający wymaga dostarczenia, instalacji i konfiguracji trzech identycznych serwerów tak aby utworzyły klaster pracy sieci informatycznej zamawiającego.
2. Serwery muszą pochodzić od tego samego producenta i spełniać poniższe wymagania.
3. Jeżeli zajdzie potrzeba, wraz z dostarczaną Infrastrukturą Serwerową, Wykonawca zobowiązany jest dostarczyć niezbędne elementy np. urządzenia i wyposażenie – kable połączeniowe, elementy mocujące, uznane przez Wykonawcę za niezbędne i umożliwiające prawidłowe działanie dostarczanej infrastruktury. Dostarczona Infrastruktura musi zapewniać bezproblemową pracę po podłączeniu do sieci informatycznej Zamawiającego
4. Wykonawca jest zobowiązany dokonać montażu dostarczonej Infrastruktury oraz oprogramowania w miejscach wskazanych przez Zamawiającego.
5. Wszystkie elementy Infrastruktury serwerowej powinny zostać zamontowane w szafie serwerowej rack, w sposób umożliwiający ich prawidłową wentylacje
6. Szczegóły dotyczące instalacji i uruchomienia Infrastruktury zostaną ustalone w trakcie Analizy Przedwdrożeniowej
7. Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont użytkowników oraz dokumentację do wszystkich oferowanych urządzeń, oprogramowania narzędziowego

(systemowego, bazodanowego, wirtualizacyjnego, backupowego itd.) wraz z dokumentami potwierdzającymi nabycia dla Zamawiającego licencji oraz nośnikami danych zawierającymi zainstalowane oprogramowanie (o ile dostarcza je producent). Wykonawca wykona również instruktaże użytkowe dla wskazanych przez Zamawiającego administratorów, z zakresu konfiguracji, obsługi i prawidłowej eksploatacji zainstalowanego Sprzętu.

8. Zaoferowane serwery musza spełniać minimalne parametry techniczne:

Lp.	Przedmiot zamówienia	Minimalne parametry wymagane
1.	**Obudowa**	Do szafy Rack 19", wysokość 1U, z zestawem szyn do mocowania w szafie;
2.	**CPU**	Zainstalowane 2 procesory w architekturze x86, dokładnie 8-rdzeniowe, o TDP nie większym niż 165W. Wynik wydajności procesora instalowanego w oferowanym serwerze wynoszący min. 178 punktów w teście SPECrate®2017_int_base, dla konfiguracji dwuprocesorowej. Wynik testu przeprowadzony dla oferowanego modelu serwera oraz zgodnego modelu procesora dostępny na stronie https://www.spec.org/;
3.	**Płyta główna**	- Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera; - Z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje; - Wyposażona w moduł zabezpieczeń zgodny z TPM 2.0; - Posiadająca 32 sloty DIMM na pamięć DDR5, obsługująca do 8TB pamięci RAM;
4.	**Pamięć RAM**	- Zainstalowane minimum 128GB pamięci RAM, pracującej w oferowanej konfiguracji z częstotliwością min. 4800MHz, w modułach o pojemności 32GB każdy;
5.	**Protekcja pamięci RAM**	- Memory mirroring, ECC, Advanced ECC lub SDDC;
6.	**GPU**	- Wbudowana karta graficzna osiągająca rozdzielczość 1920x1200 przy 60 Hz;
7.	**Zatoki dyskowe**	- Serwer wyposażony w 8 zatok dyskowych hot-plug 2.5" umożlwiających instalację dysków SSD/HDD z interfejsem SATA/SAS; - Serwer wyposażony w kontroler sprzętowy RAID pozwalający na obsługę RAID 0,1,10,5; - Serwer umożlwiający rozbudowę o 2 dyski M.2 SSD NVMe o pojemności min. 960GB działające ze sprzętowym RAID 1;
8.	**Zasilanie**	- Dwa zasilacze o mocy min. 1000W z certyfikatem Titanium.
9.	**Karty sieciowe**	- Karta Ethernet posiadająca 2 porty 10 GbE BASE-T (RJ-45) - Karta Ethernet posiadająca 2 porty 10/25GBE SFP28
10.	**Sloty PCIe**	- Serwer posiadający 2 sloty PCIe generacji 4.0 dostępne do instalacji kart rozszerzeń bez konieczność rekonfiguracji serwera; - Możliwość rozbudowy oferowanego serwera o 2 karty GPU o pamięci podręcznej min. 16GB oraz wydajności 9 TFLOPS dla obliczeń Tensor-Float 32 każda.
11.	**Dodatkowe porty**	- z przodu obudowy: 1x USB 3.0, 1x USB 2.0, 1x VGA - z tyłu obudowy: 3x USB 3.0, 1x VGA - wewnętrzne: 1 x USB 3.0
12.	**Chłodzenie**	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
13.	**Zarządzanie**	Serwer wyposażony w moduł zarządzający posiadający dedykowany port 1GbE Base-T Ethernet, pozwalający na zdalny dostęp i zarządzanie serwerem przy użyciu graficznego interfejsu Web. Moduł umożliwia:

		- monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe - dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub - dostęp do karty możliwy: • z poziomu przeglądarki webowej (GUI) • z poziomu linii komend (SSH lub IPMI) - wbudowane narzędzia diagnostyczne - zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego - obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie - wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników - przesyłanie alertów poprzez e-mail oraz SNMP - obsługa zdalnego serwera logowania (remote syslog) - wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów - monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji - konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) - zdalna aktualizacja oprogramowania (firmware) - możliwość równoczesnej obsługi przez min. 2 administratorów - wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) - możliwość instalacji karty Micro SD udostępniającej min. 4GB przestrzeni na potrzeby karty zarządzającej - Możliwość zarządzania – monitoring parametrów pracy i konfiguracja najważniejszych komponentów - z poziomu urządzania mobilnego przy użyciu dedykowanej aplikacji dostępnej na Android i/lub iOS - Możliwość monitorowania i zarządzania grupą do 200 serwerów z poziomu kontrolera zarządzania pojedynczego serwera Serwer wyposażony w wbudowany panel LCD umieszczony na froncie obudowy i pozwalający na wyświetlenie informacji o: stanie serwera, konfiguracji sieciowej karty zarządzającej, zasilaniu, temperaturze. Możliwość zarządzania – monitoring parametrów pracy i konfiguracja najważniejszych komponentów - z poziomu urządzania mobilnego przy użyciu dedykowanej aplikacji dostępnej na Android i/lub iOS. Oprogramowanie diagnostyczne producenta serwera (lub wbudowana funkcja karty zarządzającej) posiadające funkcjonalność predykcji awarii wszystkich kluczowych komponentów serwera: procesorów, pamięci RAM, dysków wewnętrznych HDD/SSD/M.2 SSD, wentylatorów, zasilaczy, kontrolerów dyskowych.
14.	**Funkcje zabezpieczeń**	- Czujnik otwarcia obudowy; - TPM 2.0;
15.	**Urządzenia hot- swap**	Dyski twarde, zasilacze, wentylatory.
16.	**Gwarancja**	- 36 miesięcy wsparcia technicznego realizowanego w trybie on-site (naprawa na w miejscu instalacji) lub poprzez wysyłkę części;

		- Usługa wsparcia technicznego świadczona przez producenta lub autoryzowany serwis producenta oferowanych urządzeń;
17.	**Inne**	- Serwer wyprodukowany zgodnie z normą ISO-9001 oraz ISO14001; - Elementy, z których zbudowane są serwery są produktami producenta tych serwerów lub są przez niego certyfikowane oraz są objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA; - Możliwość rozbudowy serwerów zgodnie z ww. wyżej specyfikacją możliwa przy użyciu dedykowanych dla danego modelu serwera komponentów oraz zachowaniu pełnego wsparcia i gwarancji producenta serwera; - Serwer fabrycznie nowy z oficjalnego kanału dystrybucyjnego w Polsce; - Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanych serwerów, nawet po wygaśnięciu 3-letniego okresu wsparcia

Serwer II - Dostawa serwera

1. **Wymagane jest dostarczenie 1 szt. serwera spełniającego poniżej opisane minimalne parametry funkcjonalne:**

Lp.	Przedmiot zamówienia	Minimalne parametry wymagane
1.	**Obudowa**	- Do szafy Rack 19", wysokość 1U, z zestawem szyn do mocowania w szafie;
2.	**CPU**	- Zainstalowany 1 procesor w architekturze x86, 16-rdzeniowy, o TDP nie większym niż 150W. Wynik wydajności procesora instalowanego w oferowanym serwerze wynoszący min. 267 punktów w teście SPECrate®2017_int_base, dla konfiguracji dwuprocesorowej. Wynik testu przeprowadzony dla oferowanego modelu serwera oraz zgodnego modelu procesora dostępny na stronie https://www.spec.org/; - Możliwość rozbudowy serwera o drugi procesor tego samego typu co zainstalowany;
3.	**Płyta główna**	- Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera; - Z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje; - Wyposażona w moduł zabezpieczeń zgodny z TPM 2.0; - Posiadająca 32 sloty DIMM na pamięć DDR5, obsługująca do 8TB pamięci RAM;
4.	**Pamięć RAM**	- Zainstalowane minimum 64GB pamięci RAM, pracującej w oferowanej konfiguracji z częstotliwością min. 4400MHz, w modułach o pojemności 32GB każdy;
5.	**Protekcja pamięci RAM**	- Memory mirroring, ECC, Advanced ECC lub SDDC;
6.	**GPU**	- Wbudowana karta graficzna osiągająca rozdzielczość 1920x1200 przy 60 Hz;
7.	**Zatoki dyskowe**	- Serwer wyposażony w 4 zatoki dyskowych hot-plug 3.5" umożlwiające instalację dysków SSD/HDD z interfejsem SATA/SAS; - Serwer wyposażony w kontroler sprzętowy RAID pozwalający na obsługę RAID 0,1,10,5; - Serwer umożlwiający rozbudowę o 2 dyski M.2 SSD NVMe o pojemności min. 960GB działające ze sprzętowym RAID 1;
8.	**Nośniki danych**	- Serwer wyposażony w 2 dyski SSD hot-plug, dedykowane do serwerów, o pojemności 960GB każdy;

9.	**Zasilanie**	- Dwa zasilacze o mocy min. 1000W z certyfikatem Titanium.
10.	**Karty sieciowe**	- Karta Ethernet posiadająca 2 porty 10 GbE BASE-T (RJ-45)
11.	**Sloty PCIe**	- Serwer posiadający 1 sloty PCIe generacji 4.0 dostępny do instalacji kart rozszerzeń bez konieczność rekonfiguracji serwera;
12.	**Dodatkowe porty**	- z przodu obudowy: 1x USB 3.0 - z tyłu obudowy: 3x USB 3.0, 1x VGA - wewnętrzne: 1 x USB 3.0
13.	**Chłodzenie**	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
14.	**Zarządzanie**	Serwer wyposażony w moduł zarządzający posiadający dedykowany port 1GbE Base-T Ethernet, pozwalający na zdalny dostęp i zarządzanie serwerem przy użyciu graficznego interfejsu Web. Moduł umożliwia: - monitorowanie podzespołów serwera: temperatura, zasilacze, - wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe - dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub - dostęp do karty możliwy: • z poziomu przeglądarki webowej (GUI) • z poziomu linii komend (SSH lub IPMI) - wbudowane narzędzia diagnostyczne - zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego - obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie - wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników - przesyłanie alertów poprzez e-mail oraz SNMP - obsługa zdalnego serwera logowania (remote syslog) - wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów - monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji - konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) - zdalna aktualizacja oprogramowania (firmware) - możliwość równoczesnej obsługi przez min. 2 administratorów - wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) - możliwość instalacji karty Micro SD udostępniającej min. 4GB przestrzeni na potrzeby karty zarządzającej - Możliwość zarządzania – monitoring parametrów pracy i konfiguracja najważniejszych komponentów - z poziomu urządzania mobilnego przy użyciu dedykowanej aplikacji dostępnej na Android i/lub iOS - Możliwość monitorowania i zarządzania grupą do 200 serwerów z poziomu kontrolera zarządzania pojedynczego serwera Możliwość zarządzania – monitoring parametrów pracy i konfiguracja najważniejszych komponentów - z poziomu urządzania mobilnego przy użyciu dedykowanej aplikacji dostępnej na Android i/lub iOS.

		Oprogramowanie diagnostyczne producenta serwera (lub wbudowana funkcja karty zarządzającej) posiadające funkcjonalność predykcji awarii wszystkich kluczowych komponentów serwera: procesorów, pamięci RAM, dysków wewnętrznych HDD/SSD/M.2 SSD, wentylatorów, zasilaczy, kontrolerów dyskowych.
15.	**Funkcje zabezpieczeń**	TPM 2.0;
16.	**Urządzenia hot-swap**	Dyski twarde, zasilacze, wentylatory.
17.	**Gwarancja**	- 36 miesięcy wsparcia technicznego realizowanego w trybie on-site (naprawa na w miejscu instalacji) lub poprzez wysyłkę części; - Usługa wsparcia technicznego świadczona przez producenta lub autoryzowany serwis producenta oferowanych urządzeń;
18.	**Inne**	- Serwer wyprodukowany zgodnie z normą ISO-9001 oraz ISO14001; - Elementy, z których zbudowane są serwery są produktami producenta tych serwerów lub są przez niego certyfikowane oraz są objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA; - Możliwość rozbudowy serwerów zgodnie z ww. wyżej specyfikacją możliwa przy użyciu dedykowanych dla danego modelu serwera komponentów oraz zachowaniu pełnego wsparcia i gwarancji producenta serwera; - Serwer fabrycznie nowy z oficjalnego kanału dystrybucyjnego w Polsce; - Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanych serwerów, nawet po wygaśnięciu 3-letniego okresu wsparcia

II.1.1 **Oprogramowanie i licencje do serwerów;**

Wymagane jest dostarczenie i wgranie oprogramowania oraz licencji na dostarczonych w ramach postępowania serwerach.

Oprogramowanie dla serwerów oraz licencje muszą spełniać poniższe minimalne parametry:

Opis	**Minimalne parametry wymagane**
Oprogramowanie – 8 szt.	- System operacyjny dedykowany do serwerów w wersji komercyjnej o zamkniętym kodzie źródłowym. - System operacyjny powinien być dostarczony w najnowszej dostępnej wersji od producenta. - System operacyjny nowy, dostarczony ze wszystkimi atrybutami legalności. - Licencja musi mieć możliwość przenoszenia na inne serwery fizyczne. - Licencja nieograniczona czasowo ani funkcjonalnie. - Licencja wieczysta dla oferowanej konfiguracji serwerów.
Bezterminowa licencja dostępowa na użytkownika – 110 licencji	- Dostarczona licencja musi być fabrycznie nowa. - Licencja musi być najnowszą wersją, możliwą do nabycia od producenta. - Licencja nieograniczona czasowo ani funkcjonalnie. - Dostarczona licencja musi posiadać cechy/atrybuty legalności.
Bezterminowa licencja dostępowa na urządzenie – 30 licencji,	- Dostarczona licencja musi być fabrycznie nowa. - Licencja musi być najnowszą wersją, możliwą do nabycia od producenta. - Licencja nieograniczona czasowo ani funkcjonalnie. - Dostarczona licencja musi posiadać cechy/atrybuty legalności.

II.1.4. Macierz - Dostawa, instalacja, konfiguracja macierzy z klastrem pracy awaryjnej, Przeniesienie danych z dotychczasowych nośników. – 1 szt.

Wykonawca dostarczy i zainstaluje macierz oraz przeprowadzi jej konfigurację wstępną zgodnie z opisem uzgodnieniu z Zamawiającym.

Macierz powinna posiadać dwa adresy IP do zarządzania – jeden adres IP na każdy z „silników" macierzy, te porty powinny zostać podłączone do przełącznika zarządzania L3.

Porty usług macierzy powinny zostać wpięte za pomocą modułów SFP28 do przełącznika dystrybucyjnego i zgodnie z konfiguracją uzgodnioną z Zamawiającym na etapie wdrożenia powinny zostać odpowiednio zaadresowane.

Dostarczona macierz powinna spełniać minimalne parametry techniczne:

Lp.	Przedmiot zamówienia	Opis przedmiotu zamówienia/ parametry wymagane
1.	Obudowa	instalacja w szafie technicznej typu RACK 19", Wysokość max. 2U.
2.	Kontrolery dyskowe	- Min. 2 kontrolery macierzowe pracujące w trybie Symmetrical Active-Active/Mesh Active-Active, to znaczy w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek (path) i portów kontrolerów w trybie bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing) nawet dla pojedynczego LUN. Dla utworzonego jednego LUN operacje I/O muszą być realizowane jednocześnie przez porty w obu kontrolerach, a generowane obciążenie (IOPS oraz Bandwidth) mają być rozłożone dla pary kontrolerów w stosunku 50/50 +/- 10%. - W przypadku zaoferowania większej ilości kontrolerów obciążenie ma być rozłożone proporcjonalnie na wszystkie kontrolery. Kontrolery muszą pozwalać na udostępnianie zasobów protokołami plikowymi oraz blokowymi. Komunikacja pomiędzy oferowanymi kontrolerami macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia; nie dopuszcza się w szczególności komunikacji z wykorzystaniem urządzeń aktywnych FC/Ethernet/Infiniband. Zamawiający dopuszcza komunikację z wykorzystaniem urządzeń aktywnych przy klastrze więcej niż 2 kontrolerów. Każdy z kontrolerów musi mieć możliwość jednoczesnej prezentacji (aktywny dostęp odczyt i zapis) wszystkich wolumenów utworzonych w logicznych ramach całego systemu dyskowego.
3.	Możliwość rozbudowy	Urządzenie musi umożliwiać podniesienie wydajności i niezawodności poprzez rozbudowę do 6 par kontrolerów, tworzących jedną logiczną macierz dyskową. Rozbudowa musi być możliwa bez konieczności wymiany zaoferowanej pary kontrolerów na nowe. Za jedną logiczną macierz uznaje się rozwiązanie, w którym zarządzanie wszystkimi kontrolerami jest możliwe z jednego interfejsu GUI, CLI. Nie dopuszcza się rozwiązań opartych o wirtualizator.

		Macierz wyłącznie do obsługi modułów pamięci NVME i w żadnej konfiguracji nie może obsługiwać przestrzeni danych użytkownika na dyskach obrotowych/talerzowych. Urządzenie musi umożliwiać dynamiczną zmianę rozmiaru woluminów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się w danym LUN. Urządzenie musi umożliwiać rozbudowę przestrzeni dyskowej o pojedynczy dysk oraz pojedynczą półkę dyskową z możliwością rozszerzenia puli dyskowej o dodany dysk/półkę bez konieczności migracji danych ani zatrzymywania pracy macierzy.
4.	Wymagana przestrzeń	Całkowita pojemność surowa RAW urządzenia musi wynosić minimum 23 TB i być zbudowana tylko i wyłącznie za pomocą dysków SSD NVMe/modułów NVMe o maksymalnej pojemności pojedynczego modułu 4 TB. Macierz musi umożliwiać rozbudowę do co najmniej 100 sztuk oferowanego typu modułów pamięci NVMe, bez wymiany lub dodawania kontrolerów macierzowych oraz bez potrzeby zakupu dodatkowych licencji. (tylko poprzez dodawanie półek dyskowych oraz kart z interfejsami i modułów NVMe). Moduły NVMe muszą posiadać redundantne interfejsy PCIe Gen 4.
5.	Procesory/Pamięć Cache	Każdy kontroler macierzy musi być oparty o wielordzeniowe procesory, minimum dwadzieścia rdzeni łącznie na kontroler. Urządzenie zbudowane z dwóch kontrolerów musi być wyposażone w co najmniej 128 GB pamięci podręcznej cache obsługującej operacje odczytu i zapisu zbudowane w oparciu o wydajną pamięć RAM. Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin.
6.	Zabezpieczenie danych	Możliwość definiowania dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej. Urządzenie musi obsługiwać poziomy RAID5, RAID6 lub RAID DP (RAID z dystrybuowaną przestrzenią zapasową typu hot-spare), oraz RAID 10.
7.	Dostępne interfejsy	Macierz musi posiadać: - minimum 8 portów 25 Gb/s lub 4 porty 100GB/s obsługujących protokół NVMe over RoCE. Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+/SFP28,QSFP28), wymaga się ich dostarczenia wraz z urządzeniem; - minimum 2 wkładki jednomodowe ze złączem LC oraz komplet patchcordów jednomodowych o długości 50cm - minimum 8 portów 10Gb/s na całą macierz. Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+/SFP28), wymaga się ich dostarczenia wraz z urządzeniem; - minimum 8 wkładek multimodowych 10Gb/s ze złączem LC oraz komplet patchcordów multimodowych o długości 50cm W oferowanej konfiguracji portów macierz musi posiadać pełną możliwość rozbudowy do wymaganej ilości modułów pamięci bez usuwania żadnego z interfejsów.

8.	Brak pojedynczego punktu awarii	Wszystkie krytyczne komponenty takie jak adaptery HBA, kontrolery dyskowe, pamięć, zasilacze i wentylatory muszą być zaprojektowane nadmiarowo: tak, aby awaria pojedynczego elementu nie wpływała na ciągłość dostępu do danych całego systemu. Komponenty te muszą być wymienialne w trakcie pracy.
9.	Prezentacja dysków logicznych o pojemności większej niż zajmowana przestrzeń dyskowa (Thin Provisioning)	Wymagana jest funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem.
10.	Protokoły dostępu do danych	Wymagane wsparcie dla NVMe over RoCE, iSCSI, NFS, CIFS. Wymagana obsługa protokołów plikowych minimum: - CIFS (minimum SMB 2.0, SMB 2.1, SMB 3.0, oraz SMB 3.1.1) - NFS (minimum NFSv3, NFSv4.0 oraz NFSv4.1). Dla zasobów udostępnianych plikowo macierz musi posiadać funkcjonalność definiowania polityk umożliwiających limitowanie ilości plików w danym katalogu oraz jego maksymalnego rozmiaru. Nie dopuszcza się realizacji funkcjonalności dostępu plikowego za pomocą dodatkowych/zewnętrznych urządzeń. Funkcjonalność ta musi być wbudowana w oprogramowanie zainstalowane w kontrolerach urządzenia. Dla zasobów plikowych macierz musi posiadać możliwość uruchomienia replikacji w trybach synchronicznym oraz asynchronicznym. Jeśli obsługa protokołów plikowych wymaga dodatkowej licencji, to nie jest wymagane jej dostarczenie wraz z urządzeniem.
11.	WORM	Dla zasobów plikowych macierz musi umożliwiać skonfigurowanie funkcji Write Once Read Many (WORM) dla utworzonego systemu plików. Każdy plik objęty ochroną WORM musi przechodzić w stan tylko do odczytu natychmiast po zapisaniu na macierzy. W stanie tylko do odczytu plik można odczytać, ale nie można go usunąć, zmodyfikować ani zmienić jego nazwy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie nie jest wymagane wraz z urządzeniem.
12.	Snapshoty	Urządzenie musi umożliwiać utworzenie 1000 kopii migawkowych (ang. snapshot) w trybie ROW (ang. Redirect on Write) dla pojedynczego wolumenu oraz minimum 4000 dla całej macierzy. Niedopuszczalne jest wykonywanie kopii w technologii COW (ang. Copy-on-Write). Rozwiązanie musi umożliwiać tworzenie grup spójności, które gwarantują spójne kopiowanie, odtwarzanie i odświeżanie wielu wolumenów naraz tj. tworzenie kopii zapasowej wielu LUNów jednocześnie. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem. Rozwiązanie musi umożliwiać hierarchiczne tworzenie kopii migawkowych (np. kopia z kopii z kopii). Dla zasobów plikowych macierz musi umożliwiać wykonywanie kopii migawkowych systemu plików z którego dane udostępniane są protokołem CIFS. Po wykonaniu kopii zmiany danych lub zapisy w systemie plików nie będą miały wpływu na dane kopii migawkowej. Musi istnieć możliwość

		zabezpieczenia kopii przed modyfikacją i usunięciem przez zadany okres czasu.
13.	Funkcje kopiujące	Tworzenie na żądanie pełnej kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z woluminu źródłowego na docelowy oraz resynchronizację danych z woluminu docelowego na źródłowy np. w sytuacji uszkodzenia danych na woluminie źródłowym. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem.
14.	Redukcja danych	Macierz musi mieć funkcjonalność deduplikacji i kompresji danych w trybie in-line zarówno dla danych blokowych jak i systemu plików. Administrator musi mieć możliwość wyłączenia mechanizmów redukcji danych dla poszczególnych woluminów LUN. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem.
15.	Replikacja danych	Macierz musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych z innymi macierzami (ten sam model/rodzina modeli) - w trybie synchronicznym i asynchronicznym - po protokołach NVMe over RoCE lub IP bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji, główek typu serwer/wirtualizator, itp. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem.
16.	Klaster wysokiej dostępności	Model oferowanej macierzy musi wspierać rozwiązanie klastra „wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów danych macierzy dla podłączonych platform software'owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po NVMe over RoCE lub IP pomiędzy 2 macierzami dostarczonymi w tym postępowaniu. Pod użytym pojęciem „wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie „wysokiej dostępności", musi wspierać klastrowanie wybranych woluminów bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną. Musi być możliwość dodawania woluminów objętych zabezpieczeniem w klastrze bez konieczności zatrzymywania replikacji. Funkcjonalność „wysokiej dostępności" musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover). Funkcjonalność „wysokiej dostępności" musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover). Funkcjonalność „wysokiej dostępności" musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback). Funkcjonalność „wysokiej dostępności" musi wspierać konfiguracje z macierzą zapasową zainstalowaną w innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem.

17.	Priorytety zadań	Macierz musi posiadać funkcjonalność zarządzania wydajnością, która dynamicznie przydziela zasoby macierzy w celu spełnienia określonych celów wydajnościowych aplikacji (QoS). Możliwość ustawiania priorytetów wydajności dla aplikacji w oparciu o zdefiniowane profile wolumenowe, dla wydajności w IOPS i przepustowości danych. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem.
18.	Kompatybilność	Model oferowanej macierzy musi znajdować się na oficjalnej liście zgodności VMware (dostępnej na stronie https://www.vmware.com/resources/compatibility/search.php). Rozwiązanie musi wspierać integrację w zakresie technologii konteneryzacji poprzez posiadanie dedykowanego sterownika Container Storage Interface (CSI).
19.	Licencje	Macierz musi być dostarczona z licencjami wymaganymi do instalacji kontrolerów z dyskami, oraz uruchomienia mechanizmów wymaganych w OPZ.
20.	Wielościeżkowość	Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: Windows Server 2019 oraz 2022, Vmware 8.0 i nowszych.
21.	Zasilanie	Urządzenie musi cechować wsparcie dla zasilania z dwóch niezależnych źródeł prądu jednofazowego o napięciu 200-240V i częstotliwości 50-60Hz poprzez nadmiarowe zasilacze typu Hot-Swap.
22.	Zarządzanie macierzą	Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy (w tym monitorowanie wydajności) oraz możliwość konfigurowania jej zasobów. Wymagana możliwość monitorowania stanu żywotności modułów NVME. Konsola graficzna musi być dostępna poprzez przeglądarkę internetową i być elementem systemu operacyjnego macierzy. Wymaga możliwość dostępu do danych wydajnościowych historycznych z poziomu GUI z co najmniej 2 lat wstecz. Macierz musi umożliwiać monitorowanie oraz przeglądanie danych historycznych z podziałem dla każdego z LUN dla min. operacji: -% trafień w cache do odczytu oraz zapisu -IOPS -średni czas odpowiedzi dla odczytu danych -średni czas odpowiedzi dla zapisu danych -przepustowość „Bandwidth" dla operacji odczytu -przepustowość „Bandwidth" dla operacji zapisu Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. Rozwiązanie musi udostępniać interfejs REST API w celu uruchamiania skryptów oraz SNMP do komunikacji z zewnętrznymi narzędziami monitorującymi.
23.	Serwisowalność	Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych. Macierz musi umożliwiać zdalne zarządzanie oraz automatyczne informowanie centrum serwisowego o awarii. Zgłoszenia usterek muszą być akceptowane zarówno drogą email jak również drogą telefoniczną.

24.	Gwarancja, wsparcie serwisowe	1) Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta na terenie RP. 2) Macierz dyskowa musi zostać objęta **minimum 60 miesięcznym okresem gwarancji** (parametr oceniany) w trybie **on-site** z gwarantowanym czasem reakcji w ciągu 60 min od momentu zgłoszenia usterki. 3) Uszkodzone dyski po awarii pozostają u Zamawiającego bez konieczności zwrotu do serwisu/producenta. 4) Zgłoszenia usterek muszą być akceptowane zarówno drogą email (w ofercie należy podać dedykowany adres email do zgłoszeń serwisowych) jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.). 5) Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta. 6) Usługi gwarancyjne muszą być świadczone przez organizację serwisową producenta sprzętu posiadającą certyfikat ISO co najmniej 9001:2015. 7) Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków: - możliwość pobierania najnowszego firmware; - dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń; - dostęp do centrum pomocy technicznej producenta; - otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware; - otrzymywanie poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy

II. 1.5. Dostawa i wdrożenie oprogramowania do wykonywania kopii zapasowych

1. **Wymagania ogólne:** Oprogramowanie musi zapewniać zaawansowane funkcje tworzenia kopii zapasowych, replikacji oraz przywracania danych dla środowisk wirtualnych, fizycznych oraz chmurowych. System powinien umożliwiać łatwe wdrożenie, zarządzanie oraz rozbudowę środowiska backupowego.
2. Oprogramowanie musi spełniać następujące funkcjonalności:

2.1. Backup maszyn wirtualnych w trybie agentless: Wymagana pełna obsługa bezagentowego tworzenia kopii zapasowych maszyn wirtualnych działających na VMware vSphere (wersje 6.0 i wyższe) oraz Microsoft Hyper-V (wersje 2016 i wyższe) oraz obsługa technologii CBT (Change Block Tracking) dla VMware oraz RCT (Resilient Change Tracking) dla Hyper-V, w celu przyspieszenia tworzenia przyrostowych kopii zapasowych.

2.2. Backup serwerów fizycznych: Obsługa backupów dla systemów Windows Server oraz Linux w oparciu o technologie przyrostowych kopii zapasowych i deduplikację na poziomie globalnym.

2.3. Backup aplikacji biznesowych: Wymagana jest natywna obsługa tworzenia kopii zapasowych dla aplikacji takich jak Microsoft Exchange, Microsoft SQL Server, Active Directory, SharePoint oraz możliwość przywracania poszczególnych elementów (np. skrzynek pocztowych, obiektów AD).

2.4. Integracja z chmurą: Oprogramowanie musi wspierać natywną integrację z popularnymi platformami chmurowymi, takimi jak Amazon AWS, Microsoft Azure oraz Wasabi, w celu przechowywania kopii zapasowych oraz replikacji danych.

2.5. Globalna deduplikacja danych: Wymagana deduplikacja na poziomie globalnym w obrębie całej infrastruktury backupowej, zarówno lokalnej, jak i chmurowej, z automatyczną kompresją danych w celu minimalizacji miejsca na dysku i transferu danych.

2.6. Wsparcie dla transportu danych przez sieć: Oprogramowanie musi wspierać przesyłanie kopii zapasowych za pomocą protokołów WAN oraz zapewniać funkcję akceleracji sieciowej (network acceleration) w celu optymalizacji transferu danych przez sieci rozległe.

2.7. Odzyskiwanie granularne: System musi zapewniać możliwość granularnego przywracania plików i

folderów z kopii zapasowej oraz natychmiastowego przywracania maszyn wirtualnych bezpośrednio z kopii zapasowej (instant VM recovery).

2.8. Replikacja maszyn wirtualnych: Oprogramowanie musi wspierać replikację maszyn wirtualnych do zdalnych lokalizacji oraz oferować funkcje automatycznego failover i manualnego failback dla przywracania dostępności systemów w razie awarii.

3. **Wymagania techniczne:** Oprogramowanie musi być zdolne do pracy na systemach Windows Server 2016, 2019 oraz 2022. Wymagana jest obsługa instalacji oprogramowania na platformach NAS takich jak QNAP, Synology oraz ASUSTOR.
4. **Licencjonowanie:** Licencjonowanie oprogramowania musi być elastyczne i obejmować możliwość licencjonowania na liczbę maszyn wirtualnych, hostów, fizycznych serwerów oraz użytkowników chmurowych. Wymagana możliwość zakupu licencji wieczystych (perpetual) oraz subskrypcyjnych (1, 3, 5 lat).
5. **Wsparcie techniczne:** Wymagana jest obsługa wsparcia technicznego 24/7 z możliwością zgłaszania problemów online oraz dostępem do regularnych aktualizacji oprogramowania

Lp.	Opis przedmiotu zamówienia/ parametry wymagane
1.	Wymagania minimalne:
2.	Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji
3.	Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012
4.	Vmware vSphere min. w wersjach v5.5-7.0.3
5.	Nutanix AHV 5.15, 5.20 (LTS)
6.	Maszyny fizyczne: Windows Server 2022, 2019, 2016, 2012R2, 2012
7.	Microsoft 365 (Exchange online, One Drive for Business, Sharepoint, Teams)
8.	Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V
9.	Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:
10.	na serwerze Windows lub Linux
11.	jako maszyna wirtualna Vmware
12.	jako maszyna wirtualna Amazon
13.	na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital
14.	Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS
15.	Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania
16.	Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).
17.	Licencjonowanie – wymaga się dostarczenia min. 6 licencji
18.	Wszystkie funkcje i komponenty oprogramowania dla środowisk Vmware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariancie wieczystym, w którym licencja nie ma terminu ważności
19.	Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 6 gniazd procesorów w obrębie środowiska
20.	W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 1 roku wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania
21.	W ramach dostawy wymagane jest dostarczenie licencji na ochronę X gniazd procesorów w hostach Vmware lub Hyper-V

22.	W ramach dostawy wymagane jest dostarczenie licencji na ochronę X maszyn fizycznych z systemem operacyjnym Windows Server lub Linux (w wersji serwerowej)
23.	W ramach dostawy wymagane jest dostarczenie licencji na ochronę X maszyn fizycznych z systemem operacyjnym Windows 10 Pro lub Ubuntu Desktop
24.	Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska
25.	Ochrona danych
26.	Oprogramowanie musi posiadać funkcje backupu i replikacji:
27.	Backup maszyn wirtualnych Vmware
28.	Replikacja maszyn wirtualnych Vmware (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
29.	Backup maszyn wirtualnych Hyper-V
30.	Replikacja maszyn wirtualnych Hyper-V (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
31.	Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych
32.	Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
33.	Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
34.	Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
35.	"Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych
36.	Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
37.	Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
38.	Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach
39.	Optymalizacja wykorzystania miejsca na dane
40.	Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
41.	Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
42.	Kompresja backupu, w tym konfigurowalny stopień kompresji
43.	Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne
44.	Spójność danych
45.	Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:
46.	Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
47.	Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
48.	Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji:
49.	Microsoft Exchange 2013, 2016, 2019
50.	Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022
51.	Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki

52.	Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V
53.	Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania
54.	Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji
55.	Przywracanie danych
56.	Oprogramowanie musi posiadać poniższe funkcje:
57.	Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
58.	Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)
59.	Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
60.	Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):
61.	Microsoft Exchange
62.	MS Active Directory
63.	MS SQL
64.	Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.
65.	Wydajność
66.	Oprogramowanie do backupu musi pozwalać na:
67.	Tworzenie backupu I replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
68.	Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
69.	Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN
70.	Akceleracje sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
71.	Wsparcie dla urządzeń oferujących dodatkową deduplikację danych
72.	Zarządzanie
73.	Oprogramowanie musi pozwalać na następujące formy zarządzania:
74.	Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
75.	Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
76.	Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania
77.	Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.
78.	Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji

Usługa odmiejscowionej kopii zapasowej danych w chmurze min. 2TB, która zapewni regularne tworzenie, przechowywanie oraz odtwarzanie kopii zapasowych danych Zamawiającego. Usługa ta ma na celu zabezpieczenie danych przed utratą, zapewniając dostępność, integralność oraz bezpieczeństwo informacji zgodnie z obowiązującymi normami i przepisami prawnymi.
Kopia w chmurze będzie służyła do przechowywania strategicznych dokumentów i baz danych Zamawiającego.

Lp.	**Przedmiot zamówienia**	**Minimalne parametry wymagane**
1.	Rodzaj chmury	Usługa musi być realizowana w chmurze prywatnej, z możliwością skalowania przestrzeni dyskowej zgodnie z potrzebami Zamawiającego.
2.	Częstotliwość wykonywania kopii zapasowych:	Kopie zapasowe muszą być wykonywane regularnie, z częstotliwością co najmniej raz dziennie. Możliwość ustawienia harmonogramu tworzenia kopii zapasowych (np. codziennie, co godzinę, co tydzień, w zależności od krytyczności danych).
3.	Szyfrowanie:	Dane muszą być szyfrowane w trakcie transferu (end-to-end encryption) oraz w spoczynku (encryption at rest) z użyciem algorytmu szyfrowania co najmniej AES-256.
4.	Przestrzeń dyskowa:	Usługa musi umożliwiać elastyczne zarządzanie przestrzenią dyskową, z możliwością zwiększenia pojemności bez przerw w działaniu usługi.
5.	Czas przechowywania kopii:	Przechowywanie kopii zapasowych przez minimum 30 dni z możliwością rozszerzenia tego okresu na żądanie Zamawiającego. Możliwość ustawienia polityk retencji (usuwania starszych kopii zapasowych po określonym czasie).
6.	Funkcjonalności usługi	Usługa musi zapewniać automatyczne tworzenie kopii zapasowych zgodnie z ustalonym harmonogramem, bez konieczności ręcznego zarządzania procesem przez użytkownika. Zamawiający musi mieć zapewniony bezpieczny i szybki dostęp do kopii zapasowych w celu ich odtworzenia w razie awarii, a także możliwość przeglądania i zarządzania kopii zapasowych przez panel zarządzania. System musi generować raporty oraz powiadomienia dotyczące statusu kopii zapasowych, w tym powiadomienia o błędach, sukcesach oraz stanie przestrzeni dyskowej.
7.	Wymagania dotyczące bezpieczeństwa	-Wymaga się, aby usługodawca spełniał najwyższe standardy bezpieczeństwa w zakresie ochrony danych, zgodnie z normami ISO/IEC 27001 lub równoważnymi. -Usługa musi spełniać wymogi przepisów prawa o ochronie danych osobowych, w tym RODO. -Możliwość przeprowadzania regularnych audytów bezpieczeństwa oraz dostępu do logów z działań związanych z tworzeniem i odtwarzaniem kopii zapasowych.
8.	Gwarancja jakości	Usługa musi być świadczona zgodnie z uzgodnionymi parametrami SLA, zapewniającymi m.in. określony czas reakcji na awarie, czas odtworzenia danych oraz dostępność usługi.
9.	Okres realizacji zamówienia	Okres świadczenia usługi wynosi 18 miesięcy.

II.1.6. Dostawa oprogramowania wraz z instalacją i wdrożeniem oprogramowania do zarządzania infrastrukturą IT dla 80 licencji wieczystych:

Lp.	**Przedmiot zamówienia**	**Minimalne parametry wymagane**
1.	Oprogramowanie:	1. Budowa modułowa, 2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. 3. Program umożliwia zmianę portu komunikacyjnego wykorzystywanego przez konsolę zarządzającą. 4. Silnik bazy danych musi być dostępny na licencji open source bez limitu ilości danych 5. Baza danych musi być darmowa i nie wymagać dodatkowego licencjonowania

2.	Monitorowanie danych użytkownika:	1. historia aktywności 2. polityka korzystania z Internetu i aplikacji 3. dostęp do zewnętrznych nośników danych, 4. grupowanie informacji w oddzielnym oknie, co umożliwia usuwanie danych użytkownika zgodne z RODO bez konieczności usunięcia informacji o stacji roboczej, 5. dostęp do danych osobowych oraz danych z monitoringu zgodnie z RODO, 6. możliwość nadawania kontom różnych poziomów dostępu oraz uprawnień do funkcji Programu, grup urządzeń i użytkowników, 7. lista kont użytkowników i administratorów, może być synchronizowana z usługą typu Active Directory, przez szyfrowane połączenia, 8. konfiguracja haseł użytkownika 9. uwierzytelnianie logowań do konsoli z wykorzystaniem weryfikacji dwuskładnikowej
3.	Funkcjonalności:	Oprogramowanie obsługuje m.in. 6 funkcjonalności: 1) Monitorowanie infrastruktury, 2) Inwentaryzacja sprzętu i oprogramowania, 3) Monitorowanie aktywności użytkowników, 4) Realizacja zdalnej pomocy użytkownikom, 5) Ochrona danych przed wyciekiem, 6) Wsparcie zarządzania czasem i analizowanie aktywności użytkowników
4.	Monitorowanie infrastruktury:	1. Wykrywanie urządzeń w sieci poprzez skanowanie ping oraz arp-ping, 2. Wizualizacja urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki, tworzenie spersonalizowanych map z możliwością zablokowania mapy urządzeń przed przypadkową edycją, 3. Serwisy TCP/IP, HTTP, POP3, SMTP, FTP i inne wraz z możliwością definiowania własnych serwisów. Monitorowanie czasu ich odpowiedzi i procent utraconych pakietów, 4. Serwery pocztowe: - program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty, - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie, - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa 5. Monitorowanie serwerów WWW i adresów URL 6. Cykliczne monitorowanie czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS 7. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail 8. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID 9. Obsługa komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych 10. Monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych - ruchu sieciowego - podłączonych stacji roboczych – graficzna prezentacja panelu switcha - ruchu generowanego przez podłączone do portów stacje robocze 11. Monitor serwisów alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie, zatrzymanie lub zrestartowanie, 12. Wyświetlanie statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa

		DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu 13. Monitorowanie stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano 14. Zarządzanie stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny 15. Wydajność systemów m.in. obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy, 16. Nakładanie na urządzenia liczników wydajności WMI oraz SNMP z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi, wyłączenie/restart komputera. 17. Administrator samodzielnie może konfigurować zdarzenia, lub wybrać zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. 18. Alarmy muszą pozwalać na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. 19. Oprogramowanie musi umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0
5.	Inwentaryzacja sprzętu i oprogramowania,	1. Automatyczne gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych, min. modelu, procesora, pamięci, płyty głównej, napędów, 2. Umożliwienie odczytów parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe. 3. Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 4. Informacja o zainstalowanych aplikacjach oraz aktualizacjach systemu 5. Zbieranie informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. 6. Możliwość wysyłania powiadomienia np. e-mailem w przypadku jakiejkolwiek zmiany na urządzeniu 7. Możliwość odczytania numeru seryjnego (klucze licencyjne). 8. Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. 9. Możliwość przeglądania informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. 10. Możliwość utworzenia listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu). 11. Możliwość wymiany plików do i ze stacją roboczą poprzez funkcję Menedżera plików. *Moduł inwentaryzacji zasobów musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:* 12. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,

		13. przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów, 14. tworzenia powiązań między zasobami a urządzeniami, 15. tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z funkcjonującą w Urzędzie Active Directory), wskazywanie osób odpowiedzialnych, 16. wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy, 17. definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości, 18. określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, 19. określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, 20. masową edycję atrybutów zasobów, 21. definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, 22. importu danych z zewnętrznego źródła (.CSV), 23. przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., 24. tworzenia powiązań między zasobami a dokumentami w relacji 1:N, 25. oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., 26. ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, 27. generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, 28. przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, 29. konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, 30. konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, 31. archiwizacji i porównywania audytów zasobów, 32. tworzenia kodów kreskowych dla zasobów, 33. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, 34. inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet, 35. możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android, 36. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), 37. definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data" z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja"). *Inwentaryzacja oprogramowania musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:* 1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. 2. Informacje o aplikacjach używanych w organizacji. 3. Tworzenie własnych wzorców aplikacji.

		4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. 5. Informacje o komputerach, na których aplikacja została wykryta. 6. Zarządzanie posiadanymi licencjami. 7. Wskazywanie osób odpowiedzialnych za licencję. 8. Wskazanie użytkowników licencji, 9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. 10. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
6.	Monitorowanie aktywności użytkowników:	1. Faktyczny czas aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy), 2. Otwarte procesy wraz z informacją o uruchomieniu na podwyższonych uprawnieniach, 3. Rzeczywiste użytkowanie programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność, 4. Informacja o edytowanych przez użytkownika dokumentach, 5. Historia pracy (cykliczne zrzuty ekranowe), 6. Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt), 7. Transfer sieciowy użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), 8. Wydruki m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program powinien mieć możliwość monitorowania kosztów wydruków, 9. Nagłówki przesyłanej w aplikacjach klienckich poczty e-mail. 10. Wykrywanie podejrzanej aktywności przez popularne „jigglery", mającej na celu symulowanie faktycznej pracy. 11. Zdefiniowanie czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury. 12. Wyszczególnienie podejrzanej aktywności w raportach. 13. Wygenerowanie alarmu i wykonanie akcji po wykryciu podejrzanej aktywności. 14. Automatyczne włączenie zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności. 15. Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). 16. Blokowania ruchu na wskazanych portach TCP/IP, 17. Blokowanie pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem, 18. Prowadzenie rejestru naruszeń blokad, 19. Wysyłanie powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,

		20. Przygotowanie zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika), 21. Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.
7.	Realizacja zdalnej pomocy użytkownikom	1. Dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika, 2. Możliwość równoczesnego podłączenia do tego samego komputera kilku administratorów. 3. Oprogramowanie powinno zawierać komunikator (czat), który umożliwi prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów. Czat powinien pozwalać na: 4. zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej 5. rozmowy między „zwykłymi" użytkownikami 6. przesyłanie plików między rozmówcami w trybie online 7. tworzenie pokojów tematycznych, rozmów grupowych 8. oznaczanie kontaktów jako „ulubionych" na liście kontaktów 9. uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku, 10. Administrator powinien mieć możliwość tworzenia szkiców i archiwizowania komunikatów. Moduł pomocy zdalnej powinien umożliwiać: 11. pobieranie listy użytkowników z Active Directory, 12. wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym, 13. zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont, 14. zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez system zarządzania regułami widoczności zgłoszeń, 15. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń, 16. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy, 17. tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO, 18. automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników, 19. definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji, 20. przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii, 21. procesowanie zgłoszeń użytkowników z wiadomości e-mail, 22. eksportowania listy zgłoszeń do plików CSV i XLSX, 23. integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0, 24. tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń, 25. wykonywanie operacji na wielu zgłoszeniach równocześnie,

		26. dołączanie załączników do zgłoszeń, 27. rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, 28. szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, 29. wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia, 30. zrzuty ekranowe (podgląd pulpitu), 31. zdalną modyfikację rejestrów, 32. dystrybucję oprogramowania przez Agenty, 33. dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), 34. możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu, 35. możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy, 36. planowanie nieobecności pracowników helpdesk, 37. obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem, 38. generowanie raportów obsługi helpdesk, 39. zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu), 40. zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), 41. wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.
8.	Ochrona danych przed wyciekiem	Blokowanie urządzeń i nośników danych: 1. możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. 2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. 3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. 4. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. 5. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender. 6. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker. 7. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker. 8. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu. 9. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu. 10. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender 11. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM. Zarządzanie prawami dostępu do urządzeń: 1) Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.

		2) Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. 3) Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników. 4) Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. 5) Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane. Audyt operacji na plikach na urządzeniach przenośnych: 1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. 2. Podłączenie/odłączenie urządzenia przenośnego. 3. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. 4. Definiowanie reguł monitorowanych folderów w postaci list. Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.) Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.
9.	Zarządzanie czasem i analizowanie aktywności użytkowników	1. Możliwość oznaczenia sesji aktywności jako czas prywatny gdy pracownik wykonuje czynności prywatne na sprzęcie firmowym. 2. Użytkownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. 3. Zastosowane reguły powinny pozwalać zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. Dostęp powinien być realizowany przez przeglądarkę internetową, a strona powinna być wyświetlana w trybie jasnym lub ciemnym. 4. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. 5. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem. 6. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu. 7. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników. 8. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych. 9. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne. 10. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy. 11. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie). 12. Wskaźnik czasu poświęconego na aktywność produktywną. 13. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail. 14. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Rozrywka - predefiniowana lista kategorii z możliwością edycji. 15. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.
10.	Gwarancja, wsparcie serwisowe	1. Wsparcie techniczne przez min. rok od dnia podpisania protokołu odbioru 2. W ramach wsparcia technicznego możliwość instalowania wszelkich aktualizacji oprogramowania, które zostaną wydane w czasie

		obowiązywania wsparcia, w tym aktualizacji obejmujących przejście na wyższą wersję oprogramowania. 3. Telefoniczne i mailowe wsparcie techniczne dla oprogramowania 4. Dokonywanie przez Producenta szczegółowej analizy zgłoszonych przypadków (logów). 5. Świadczenie przez Producenta pomocy w formie sesji zdalnych. 6. Czas reakcji na zgłoszenie nie dłuższy niż następny dzień roboczy. 7. Możliwość przedłużenia wsparcia o kolejny rok 8. Możliwość rozszerzenia oprogramowania o dodatkowe licencje i moduły

II. 1.7. Wdrożenie usług domeny do zarzadzania siecią i zasobami komputerowymi:

1. W ramach wdrożenia usług domeny do zarządzania siecią i zasobami komputerowymi Zamawiający wymaga:
    a. zaplanowania wdrożenia oraz struktury 80 użytkowników,
    b. Planowanie i przygotowanie środowiska informatycznego
    c. Instalacja systemu operacyjnego na serwer
    d. Instalacja roli domeny
    e. Konfiguracja kontrolera domeny
    f. Weryfikacja konfiguracji domeny
    g. Tworzenie jednostek organizacyjnych
    h. Konfiguracja polityk grupowych
    i. Przeszkolenia administratora sieci informatycznej,

II.1.8. Dostawa i instalacja i konfiguracja przełącznika dystrybucyjnego (zwany powyżej L3) – 1 szt.

Parametr	**Charakterystyka (Wymagane minimalne)**
Przełącznik posiada:	1. min. 48 portów 1/10/25GE SFP28 bezpośrednio w obudowie przełącznika lub na karcie liniowej przełącznika modularnego 2. min. 6 portów definiowanych za pomocą wkładek QSFP, bezpośrednio w obudowie przełącznika lub na karcie liniowej, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps 3. Pamięć systemu min. 24 GB 4. Dysk SSD min. 64 GB
Parametry wydajnościowe:	1. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3 2. Obsługiwana łączna przepływność (pasmo) min. 3,6 Tbps 3. Obsługiwana łączna przepustowość pakietowa przełącznika min. 1,6 bpps 4. opóźnienie przełączania pakietów nie większe niż 2 µs .
Funkcjonalność warstwy L2:	1. Trunking IEEE 802.1Q VLAN; 2. Wsparcie dla min. 3967 sieci VLAN; 3. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN 4. Wsparcie sprzętowe dla minimum 256 tysięcy adresów MAC 5. IEEE 802.1s Multiple Spanning Tree (MST) 6. Statyczny i dynamiczny NAT 7. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree 8. Internet Group Management Protocol (IGMP)
Funkcjonalność warstwy L3	1. Sprzętowe przełączanie pakietów w warstwie L3 2. Routing w oparciu o trasy statyczne 3. Routing w oparciu o OSPF, BGP 4. Wsparcie sprzętowe dla minimum 896 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP 5. Wsparcie dla IPv4 multicast w oparciu o protokół PIM-SM Sparse Mode I tryb SSM (Source Specific Multicast) 6. Wsparcie dla IGMPv3 oraz MSDP 7. Wsparcie sprzętowe dla minimum 32,000 tras multicastowych

	8. Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking) 9. Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP) 10. Minimum 1000 wejściowych oraz min. 1000 wyjściowych wpisów dla ACL - access control list
Wsparcie mechanizmów bezpieczeństwa w sieci:	1. Wsparcie ACL 2. Snooping 3. ARP Inspection
Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:	1. Port zarządzający 100/1000 Mbps; 2. Port konsoli CLI; 3. Ping 4. Traceroute.
Akcesoria:	1. 2 szt. wkładek QSFP-100G-LR4-S 2. 2 szt. patchcord LCLC-SM-50CM 3. 15 szt. składek SFP-10G-SR 4. 6 szt. wkładek SFP+ SFP-25G-SR.
Zasilanie	1. 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej.
Obudowa	1. maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19". W wypadku zastosowania przełącznika modularnego dopuszcza się większy rozmiar urządzenia (jednak nie większy niż 2U).
Gwarancja:	1. min. 60 miesięcy 2. Gwarancja obejmuje wszystkie części składowe urządzenia.
Serwis	1. Świadczony na miejscu u Zamawiającego 2. Opieka serwisowa 24 godziny na dobę 7 dni w tygodniu. 3. Czas reakcji na zgłoszenie awarii max. do 60 min. 4. Wymagany czas naprawy awarii 24 godziny od momentu zgłoszenia. W przypadku niemożliwego usunięcia awarii w przeciągu 24 godz. Wykonawca jest zobowiązany dostarczyć urządzenie zamienne, o parametrach nie gorszych, na czas usunięcia awarii. 5. Uszkodzone nośniki danych pozostają u Zamawiającego. 6. Kontakt z pracownikami serwisu będzie prowadzony w języku polskim.

II.1.9. Dostawa i wdrożenie zarządzalnych przełączników sieciowych do utworzenia rdzenia sieci LAN – 6 szt.

LP.	Przedmiot zamówienia	Opis przedmiotu zamówienia/ parametry wymagane
1.	Typ i liczba portów	48 portów 10/100/1000BaseT RJ-45 + uplink 4x10G SFP
2.	Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:	- Gigabit Ethernet 1000Base-SX, - Gigabit Ethernet 1000Base-LX/LH, - 10Gigabit Ethernet 10GBase-SR, - 10Gigabit Ethernet 10GBase-LR, - • 10Gigabit Ethernet typu twinax (SFP+ - SFP+)
3.	Urządzenie posiada funkcjonalność zarządzania przez 1 adres IP grupą (klastrem)	do 8 urządzeń pochodzących z tej samej rodziny przełączników połączonych portami uplinkowymi,
4.	Zasilanie i chłodzenie	- Urządzenie wyposażone jest w wbudowany zasilacz AC230V
Parametry wydajnościowe		
5.	Przepustowość przełącznika	min. 176 Gb/s (full duplex),

	(switching bandwidth)	
6.	Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3	min. 77.38 Mpps
7.	Pamięć DRAM	Min. 512 MB
8.	Pamięć flash	256 MB
9.	Wielkość bufora pakietów	1.5 MB
10.	Obsługa	- 256 aktywnych sieci VLAN - 15000 adresów MAC - 16 statycznych tras IPv4 - 16 statycznych tras IPv6 - 64 interfejsów SVI L3 - Obsługa MTU-L3 9198B - Obsługa ramek Ethernet Jumbo 10240B - 1024 grupy IGMP - 6 połączeń zagregowanych typu „port channel" - 16 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP - Ilość wpisów w listach kontroli dostępu Security ACL – 600 - • ilość wpisów w listach kontroli dostępu QoS ACL – 600
11.	Porty dostępowe przełącznika posiadają zgodność ze standardem	standard IEEE 802.3az EEE (Energy Efficient Ethernet)
12.	Obsługa protokołu	NTP, LLDP i LLDP-MED
13.	Obsługa	IGMPv1/2/3 i MLDv1/2 Snooping
14.	Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC	Tak
15.	Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad	Tak
16.	Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego	Tak
17.	Możliwość uruchomienia funkcji serwera DHCP	Tak

18.	Mechanizmy związane z bezpieczeństwem sieci:	- Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level), - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL, - Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X, - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, - Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X, - Możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem (multidomain authentication), - Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, - Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www), - Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, - Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, - Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP), - Funkcja Private VLAN,
19.	Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:	- sprawdzanie autentyczności oprogramowania przed uruchomieniem urządzenia, - bezpieczna sekwencja uruchamiania, - sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
20.	Mechanizmy związane z zapewnieniem jakości usług w sieci:	- Implementacja 4 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, - Implementacja algorytmu Shaped Round Robin dla obsługi kolejek, - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), - Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, - Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z możliwością skonfigurowania minimum 64 różnych ograniczeń, - Kontrola sztormów dla ruchu broadcast/multicast/unicast, - Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS)

		oraz IP ToS/DSCP;
21.	Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6	Tak
22.	Przełącznik umożliwia lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizm SPAN z możliwością obsługi do 4 sesji monitorujących,	Tak
23.	Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.),	Tak
24.	Obsługa protokołu sFlow dla wszystkich portów fizycznych uplinkowych i downlinkowych dla ruchu w kierunku wejściowym i wyjściowym z możliwością skonfigurowania 2 różnych kolektorów ruchu sFlow,	Tak
Zarządzanie		
25.	Port konsoli,	Tak
26.	Dostęp bezprzewodowy Bluetooth do interfejsu zarządzającego	Tak

	urządzenia (telnet, ssh) przez zastosowanie zewnętrznego urządzenia Bluetooth podłączonego do portu USB przełącznika,	
27.	Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,	Tak
28.	Obsługa protokołów	SNMPv3, SSHv2, https, syslog,
29.	Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia	Tak/podać
30.	Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki;	Tak/podać
31.	Możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU	Tak/podać
32.	Akcesoria	1. 5 szt. wkładek SFP-10G-SR 2. 5 szt. Patchord LCLC-MM-OM3-50CM
Warunki Gwarancji i serwisu		
33.	Gwarancja dla wszystkich urządzeń należących do przedmiotu zamówienia min 12 m-ce liczone od dnia podpisania protokołu odbioru	
34.	Gwarancja obejmuje wszystkie części składowe urządzenia.	
35.	Gwarantowany czas naprawy awarii 24 godziny od momentu zgłoszenia. W przypadku niemożliwego usunięcia awarii w przeciągu 24 godz. Wykonawca jest zobowiązany dostarczyć urządzenie zamienne, o parametrach nie gorszych, na czas usunięcia awarii.	
36.	Świadczony na miejscu u Zamawiającego	

37.	Opieka serwisowa 24 godziny na dobę 7 dni w tygodniu.
38.	Czas reakcji na zgłoszenie max. 60 min, rozpoczęcie naprawy w ciągu 24 godz. od zgłoszenia.
39.	Kontakt z pracownikami serwisu będzie prowadzony w języku polskim.

II.1.10. Dostawa, instalacja oraz podłączenie zasilacza awaryjnego UPS z kartą SNMP

W ramach rozbudowy sieci informatycznej Zamawiającego niezbędne jest zapewnienie dodatkowego zasilania awaryjnego gwarantującego ciągłość pracy podczas zaniku prądu w sieci. Wykonawca w ramach realizacji zamówienia dostarczy i zainstaluje w serwerowni Zamawiającego w szafie rac zasilacz awaryjny spełniający poniższe minimalne wymagania techniczne:

LP.	Przedmiot zamówienia	Opis przedmiotu zamówienia/ parametry wymagane
1.	Moc	min. 3000VA/2700W
2.	Obudowa	Możliwość montażu na stojąco jak i w szafie rack 19"
3.	Faza	1 faza z uziemieniem
4.	Typ baterii	12V/9AH
5.	Ilość baterii	min. 4
6.	Czas ładowania	max. 4 godzin regeneracji do 90% pojemności
	Wejście	
7.	Napięcie Zakres napięcia Zakres częstotliwości	208/220/230/240 VAC 110-300 VAC ± 5% przy 50% obciążenia 160-300 VAC ± 5% przy 100% obciążenia 40/70 Hz (automatyczne wykrywanie)
	Wyjście	
8.	Napięcie wyjściowe Regulacja napięcia AC (tryb baterii) Zakres częstotliwości (tryb baterii) Max czas przełączenia UPS w tryb zasilania akumulatorowego Kształt fali (tryb baterii)	208/220/230/240 VAC ±1% 57~63 Hz lub 50 Hz ± 0.1 Hz max. 4 ms Czysta fala sinusoidalna
9.	Możliwość wymiany baterii podczas pracy	Tak
10.	Zabezpieczenie przed przeciążeniem, rozładowaniem i przeładowaniem	Tak
	Wskaźniki	
11.	Wyświetlacz LCD	Poziom obciążenia, poziom naładowania akumulatora, tryb AC, tryb akumulatora, tryb obejścia i wskaźnik usterki
	Alarm:	
12.	Tryb baterii	Dźwięk co 4 s
13.	Niski poziom naładowania baterii	Dźwięk co 1 s
14.	Przeciążenie	Dźwięk dwa razy na sekundę
15.	Usterka	Ciągły sygnał dźwiękowy
	Środowisko	
16.	Działanie w warunkach wilgotności	20-90% wilgotności względnej przy 0-40°C (bez kondensacji)
17.	Poziom hałasu	Mniej niż 50 dBA w odległości 1 metra

18.	Czas podtrzymania w zależności od obciążenia	min. 11,5 min przy 50% obciążeniu bez dodatkowych akumulatorów
19.	Wbudowany stabilizator AVR	Tak
20.	Automatyczny restart podczas przywracania napięcia AC	Tak
21.	Funkcja zimnego startu	Tak
22.	Ładowanie w trybie wyłączenia	Tak
23.	Wbudowany port komunikacyjny	USB, RJ, SNMP
24.	Karta SNMP	Tak
25.	Złącze wejście AC Złącze wyjścia AC	min. 1x IEC 320 x14 min. 1x IEC 320 C19 min. 6x IEC 320 C13
	Zarządzanie	
26.	Interfejs RS 232/USB	Wsparcie Windows 2000/2003/XP/Vista/2008, Windows 7,8,10 Linux i MAC
	Warunki Gwarancji i serwisu	
27.	Gwarancja dla wszystkich urządzeń należących do przedmiotu zamówienia 24 m-ce liczone od dnia podpisania protokołu odbioru	Tak/podać
28.	Gwarancja obejmuje wszystkie części składowe urządzenia.	Tak/podać
29.	Gwarantowany czas naprawy awarii 24 godziny od momentu zgłoszenia. W przypadku niemożliwego usunięcia awarii w przeciągu 24 godz. Wykonawca jest zobowiązany dostarczyć urządzenie zamienne, o parametrach nie gorszych, na czas usunięcia awarii.	Tak/podać
30.	Świadczony na miejscu u Zamawiającego	Tak/podać
31.	Opieka serwisowa 24 godziny na dobę 7 dni w tygodniu.	Tak/podać
32.	Czas reakcji na zgłoszenie max. 60 min, rozpoczęcie naprawy w ciągu 24 godz. od zgłoszenia.	Tak/podać
33.	Kontakt z pracownikami serwisu będzie prowadzony w języku polskim.	Tak/podać

II.1.11. Dostawa wraz z montażem i uruchomieniem dysków 12TB przeznaczonych do wykonywania kopii zapasowych – 5 szt.

W ramach rozbudowy urządzenia typu NAS, posiadanego przez Zamawiającego, Wykonawca zobowiązany jest dostarczyć i zainstalować 5 identycznych dysków twardych o pojemności12TB, przeznaczonych do pracy w systemach NAS, w technologii SATA.

LP.	Przedmiot zamówienia	Minimalne parametry wymagane
1	Pojemność	12 TB
2	Interfejs	SATA III (6 Gb/s)
3	Rozmiar	3,5''
4	Prędkość obrotowa	7200 RPM

5	Pamięć cache	256 MB
6	Kompatybilność	Kompatybilność z systemami NAS, RAID, systemami przechowywania danych o wysokiej wydajności
7	Gwarancja	36 miesięcy gwarancji

II.1.12.Szkolenie ASI tworzenie i administracja sieci VLAN:

1. **Przedmiot zamówienia**: Przedmiotem zamówienia jest przeprowadzenie szkolenia dla Administratora Sieci Informatycznej (ASI) z tworzenia i administracji sieci VLAN dla 1 osoby
2. **Cel szkolenia**: Celem szkolenia jest zapoznanie uczestnika z zagadnieniami dotyczącymi tworzenia i zarządzania wirtualnymi sieciami lokalnymi (VLAN) w celu podziału sieci komputerowej na segmenty. Dzięki zastosowaniu VLAN możliwe jest zwiększenie bezpieczeństwa sieci poprzez ograniczenie ryzyka ataku na całą sieć, a także efektywniejsze zarządzanie ruchem sieciowym w organizacji.
3. **Zakres merytoryczny szkolenia:** Zakres szkolenia musi obejmować minimum:
   a. Podstawy sieci komputerowych LAN:
      - Architektura sieci LAN.
      - Elementy składowe sieci lokalnej.

   b. Wirtualne sieci LAN (VLAN):
      - Definicja i korzyści z zastosowania VLAN.
      - Typy VLAN: Data VLAN, Voice VLAN, Management VLAN, itp.

   c. Koncepcje segmentacji sieci z użyciem VLAN:
      - Separacja ruchu sieciowego.
      - Zwiększenie bezpieczeństwa poprzez izolację sieci.

   d. Praktyczne aspekty tworzenia VLAN:
      - Podział sieci na segmenty VLAN.
      - Konfiguracja podstawowych ustawień VLAN na przełącznikach sieciowych.

   e. Case Study: Przykłady zastosowania VLAN w urzędach:
      - Wprowadzenie do struktury sieci urzędu.
      - Analiza potencjalnych zagrożeń i sposoby ich minimalizacji.

   f. Konfiguracja trunkingu VLAN:
      - Definicja trunkingu.
      - Konfiguracja łącz trunkingowych pomiędzy przełącznikami.
      - Zarządzanie VLAN na poziomie warstwy 2 i 3.

   g. VLAN Routing (Inter-VLAN Routing):
      - Konfiguracja rutingu między VLAN-ami.
      - Przykłady zastosowań i korzyści.

   h. Zabezpieczenia VLAN:
      - Techniki zapobiegania atakom typu VLAN hopping.
      - Implementacja Access Control Lists (ACL) w celu zabezpieczenia segmentów sieci.

   i. Monitorowanie i zarządzanie VLAN:
      - Narzędzia do monitorowania ruchu w sieciach VLAN.
      - Praktyczne aspekty zarządzania sieciami VLAN.

   j. Warsztaty praktyczne:
      - Konfiguracja VLAN na sprzęcie sieciowym (ćwiczenia).
      - Symulacja scenariuszy ataków na sieć i sposoby ich zapobiegania.

   k. Najczęstsze problemy i ich rozwiązywanie:
      - Omówienie typowych problemów związanych z VLAN.
      - Sposoby diagnozowania i rozwiązywania problemów

4. **Forma i organizacja szkolenia**:
   1) Szkolenie powinno być przeprowadzone w formie warsztatów stacjonarnych, z wykorzystaniem prezentacji multimedialnych, studiów przypadków oraz ćwiczeń praktycznych
   2) Zamawiający oświadcza, że udostępni Wykonawcy miejsce na czas przeprowadzenia szkolenia
5. **Termin realizacji**:
   1) Wykonawca przekaże Zamawiającemu agendę szkolenia wraz z proponowanym terminem przeprowadzenia szkolenia uwzględnionym w Harmonogramie wdrożenia

2) Przewidywany czas szkolenia – min. 2 dni po 8 godz.

6. **Wymagania wobec wykonawcy:** Wykonawca lub każda wskazana przez Wykonawcę osoba do prowadzenia szkolenia posiada co najmniej 2-letnie doświadczenie zawodowe (praktyczne i/lub dydaktyczne) w zakresie wystąpień/szkoleń/prelekcji o tematyce bezpieczeństwa informacji. Na potwierdzenie doświadczenia Wykonawca dołączy do oferty Referencje potwierdzające realizację minimum 2 wystąpień/szkoleń/prelekcji o związanych z tematyką bezpieczeństwa informacji przeprowadzonych w okresie ostatnich 3 lat od złożenia oferty, a jeżeli ten okres jest krótszy to w tym okresie
7. **Materiały szkoleniowe:** Wykonawca zobowiązany jest do przygotowania i dostarczenia uczestnikowi materiałów szkoleniowych w formie drukowanej oraz elektronicznej
8. **Ocena efektywności szkolenia:** Po zakończeniu szkolenia, wykonawca przeprowadzi test wiedzy oraz ankietę ewaluacyjną w celu oceny efektywności szkolenia i zadowolenia uczestnika.
9. **Certyfikat:** Szkolenie powinno zakończyć się certyfikatem imiennym potwierdzającym odbycie się szkolenia.

II.1.13.Szkolenie ASI tworzenie i administracja serwerami Windows

1. **Przedmiot zamówienia**: Przedmiotem zamówienia jest przeprowadzenie szkolenia dla Administratora Sieci Informatycznej (ASI) z tworzenia i administracji serwerami Windows dla 1 osoby
2. **Cel szkolenia**: Celem szkolenia jest zapoznanie uczestnika z kluczowymi zagadnieniami związanymi z administracją serwerami opartymi na platformie Windows Server. Uczestnik powinien nauczyć się zarządzać zasobami, użytkownikami, oraz konfiguracją serwerów w środowisku sieciowym
3. **Zakres merytoryczny szkolenia:** Zakres szkolenia musi obejmować minimum:
   a. Wprowadzenie do szkolenia i zapoznanie z harmonogramem.
   b. Instalacja i konfiguracja Windows Server:
      - Przegląd edycji Windows Server.
      - Instalacja systemu operacyjnego.
      - Podstawowe konfiguracje po instalacji.
   c. Zarządzanie użytkownikami i grupami:
      - Tworzenie i zarządzanie kontami użytkowników.
      - Konfiguracja grup i uprawnień.
   d. Zarządzanie zasobami i uprawnieniami:
      - Udostępnianie folderów i drukarek.
      - Konfiguracja uprawnień NTFS.
   e. Zarządzanie politykami grupowymi (GPO):
      - Wprowadzenie do GPO.
   f. Monitorowanie i utrzymanie serwerów:
      - Przegląd narzędzi monitorujących.
      - Diagnostyka i rozwiązywanie problemów.
   g. Zarządzanie rolami i funkcjami serwera:
      - Instalacja i konfiguracja ról serwera.
      - Zarządzanie funkcjami serwera.
   h. Konfiguracja usług sieciowych:
      - DHCP i DNS: podstawy i konfiguracja.
      - Zarządzanie usługami sieciowymi.
   i. Backup i odtwarzanie systemów:
      - Strategie backupu.
      - Konfiguracja usług backupu i odtwarzania danych.
   j. Wprowadzenie do wirtualizacji z Hyper-V:
      - Konfiguracja roli Hyper-V.
4. **Forma i organizacja szkolenia**:
   1) Szkolenie powinno być przeprowadzone w formie warsztatów stacjonarnych, z wykorzystaniem prezentacji multimedialnych, studiów przypadków oraz ćwiczeń praktycznych
   2) Zamawiający oświadcza, że udostępni Wykonawcy miejsce na czas przeprowadzenia szkolenia
5. **Termin realizacji**:

1) Wykonawca przekaże Zamawiającemu agendę szkolenia wraz z proponowanym terminem przeprowadzenia szkolenia uwzględnionym w Harmonogramie wdrożenia
2) Przewidywany czas szkolenia – min. 2 dni po 8 godz.

6. **Wymagania wobec wykonawcy:** Wykonawca lub każda wskazana przez Wykonawcę osoba do prowadzenia szkolenia posiada co najmniej 2-letnie doświadczenie zawodowe (praktyczne i/lub dydaktyczne) w zakresie wystąpień/szkoleń/prelekcji o tematyce bezpieczeństwa informacji. Na potwierdzenie doświadczenia Wykonawca dołączy do oferty Referencje potwierdzające realizację minimum 2 wystąpień/szkoleń/prelekcji o związanych z tematyką bezpieczeństwa informacji przeprowadzonych w okresie ostatnich 3 lat od złożenia oferty, a jeżeli ten okres jest krótszy to w tym okresie
7. **Materiały szkoleniowe:** Wykonawca zobowiązany jest do przygotowania i dostarczenia uczestnikowi materiałów szkoleniowych w formie drukowanej oraz elektronicznej
8. **Ocena efektywności szkolenia:** Po zakończeniu szkolenia, wykonawca przeprowadzi test wiedzy oraz ankietę ewaluacyjną w celu oceny efektywności szkolenia i zadowolenia uczestnika.

Certyfikat: Szkolenie powinno zakończyć się certyfikatem imiennym potwierdzającym odbycie się szkolenia

II.1.14. Szkolenie ASI z domeny do zarządzania siecią I zasobami komputerowymi

1. **Przedmiot zamówienia**: Przedmiotem zamówienia jest przeprowadzenie szkolenia dla Administratora Sieci Informatycznej (ASI) z wdrożonej usługi do zarządzania tożsamościami użytkowników dla administratora – 1 osoba.
2. **Cel szkolenia**: Celem szkolenia dla ASI (Administratora Systemów Informatycznych) z zakresu zarządzania siecią i zasobami komputerowymi jest nabycie umiejętności niezbędnych do efektywnego zarządzania infrastrukturą IT w urzędzie.
3. **Zakres merytoryczny szkolenia:** Zakres szkolenia musi obejmować minimum:
   a. Instalacja i konfiguracja kontrolerów domeny, w tym omówienie zasad wdrożenia.
   b. Zarządzanie obiektami, w tym min. zarządzanie kontami użytkowników, zarządzanie grupami, zarządzanie obiektami typu komputer,
   c. Zarządzanie zaawansowaną infrastrukturą domeny w tym konfiguracja relacji zaufania w domenie,
   d. Wdrażanie i zarządzanie lokacjami i repliką w domenie w tym min. Omówienie replikacji usług, Konfigurowanie lokacji usługi, Konfigurowanie i monitorowanie replikacji usług
   e. Wdrażanie zasad grupy w tym min. wprowadzenie do zasad grupy, wdrażanie i zarządzanie obiektami GPO (Group Policy Object), konfiguracja zakresu i przetwarzania obiektów GPO, rozwiązywanie problemów z GPO
   f. Zarządzanie ustawieniami użytkowników za pomocą zasad grupy w tym min. wdrażanie szablonów administracyjnych, konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów
4. **Forma i organizacja szkolenia**:
   1) Szkolenie powinno być przeprowadzone w formie warsztatów stacjonarnych, z wykorzystaniem prezentacji multimedialnych, studiów przypadków oraz ćwiczeń praktycznych
   2) Zamawiający oświadcza, że udostępni Wykonawcy miejsce na czas przeprowadzenia szkolenia
5. **Termin realizacji**:
   1) Wykonawca przekaże Zamawiającemu agendę szkolenia wraz z proponowanym terminem przeprowadzenia szkolenia uwzględnionym w Harmonogramie wdrożenia
   2) Przewidywany czas szkolenia – min. 2 dni po 8 godz.
6. **Wymagania wobec wykonawcy:** Wykonawca lub każda wskazana przez Wykonawcę osoba do prowadzenia szkolenia posiada co najmniej 2-letnie doświadczenie zawodowe (praktyczne i/lub dydaktyczne) w zakresie wystąpień/szkoleń/prelekcji o tematyce bezpieczeństwa informacji. Na potwierdzenie doświadczenia Wykonawca dołączy do oferty Referencje potwierdzające realizację minimum 2 wystąpień/szkoleń/prelekcji o związanych z tematyką bezpieczeństwa informacji przeprowadzonych w okresie ostatnich 3 lat od złożenia oferty, a jeżeli ten okres jest krótszy to w tym okresie
7. **Materiały szkoleniowe:** Wykonawca zobowiązany jest do przygotowania i dostarczenia uczestnikowi materiałów szkoleniowych w formie drukowanej oraz elektronicznej
8. **Ocena efektywności szkolenia:** Po zakończeniu szkolenia, wykonawca przeprowadzi test wiedzy oraz ankietę ewaluacyjną w celu oceny efektywności szkolenia i zadowolenia uczestnika.
9. **Certyfikat:** Szkolenie powinno zakończyć się certyfikatem imiennym potwierdzającym odbycie się

szkolenia

II.1.15. Szkolenie ASI Budowa klastra Hyper-V

1. **Przedmiot zamówienia**: przeprowadzenie specjalistycznego szkolenia dla ASI z budowy klastra Hyper-V – 1 osoba.
2. **Cel szkolenia**: Celem szkolenia jest nauczenie uczestnika budowy i zarządzania klastrami hostów funkcji Hyper-V w sieci szkieletowej urzędu. Pozwala zbudować ekonomiczne i łatwe w zarządzaniu środowisko wirtualizacji poprzez połączenie zasobów obliczeniowych, pamięci masowej i sieciowych na jedną platformę sprzętową.
3. **Zakres merytoryczny szkolenia:** Zakres szkolenia musi obejmować minimum:
   a. Wprowadzenie do Hyper-V i klastrów:
   - Omówienie wirtualizacji.
   - Podstawy Hyper-V i korzyści z użycia klastrów.

   b. Instalacja i konfiguracja Hyper-V:
   - Instalacja roli Hyper-V na serwerze.
   - Konfiguracja podstawowych ustawień Hyper-V.

   c. Wprowadzenie do zarządzania klastrami:
   - Omówienie architektury klastra.
   - Wymagania sprzętowe i programowe dla klastra.

   d. Przerwa na kawę.
   e. Konfiguracja i uruchomienie klastra Hyper-V:
   - Tworzenie klastra Hyper-V.
   - Konfiguracja węzłów klastra.

   f. Zarządzanie zasobami klastra:
   - Przypisywanie zasobów do klastra.
   - Zarządzanie pamięcią i zasobami CPU w klastrze.

   g. Praktyczne ćwiczenia: Budowa klastra:
   - Konfiguracja i zarządzanie maszynami wirtualnymi w klastrze.
   - Migracja maszyn wirtualnych między węzłami klastra.

   h. Zaawansowane Zarządzanie Klastrem Hyper-V
   - Instalacja i konfiguracja VMM.
   - Integracja VMM z Hyper-V.

   i. Zarządzanie maszynami wirtualnymi w VMM:
   - Tworzenie, konfiguracja i migracja VM w VMM.
   - Automatyzacja zadań zarządzania VM.

   j. Zaawansowane funkcje klastra:
   - High Availability i Disaster Recovery w klastrach Hyper-V.
   - Zarządzanie zasobami w kontekście awarii.

   k. Monitorowanie i optymalizacja klastra:
   - Narzędzia do monitorowania wydajności klastra.
   - Optymalizacja pracy maszyn wirtualnych.

   l. Backup i odzyskiwanie danych w klastrze:
   - Tworzenie kopii zapasowych VM.
   - Odzyskiwanie VM po awarii.
4. **Forma i organizacja szkolenia**:
   1) Szkolenie powinno być przeprowadzone w formie warsztatów stacjonarnych, z wykorzystaniem prezentacji multimedialnych, studiów przypadków oraz ćwiczeń praktycznych
   2) Zamawiający oświadcza, że udostępni Wykonawcy miejsce na czas przeprowadzenia szkolenia
5. **Termin realizacji**:
   1) Wykonawca przekaże Zamawiającemu agendę szkolenia wraz z proponowanym terminem przeprowadzenia szkolenia uwzględnionym w Harmonogramie wdrożenia
   2) Przewidywany czas szkolenia – min. 2 dni po 8 godz.
6. **Wymagania wobec wykonawcy:** Wykonawca lub każda wskazana przez Wykonawcę osoba do prowadzenia szkolenia posiada co najmniej 2-letnie doświadczenie zawodowe (praktyczne i/lub dydaktyczne) w zakresie wystąpień/szkoleń/prelekcji o tematyce bezpieczeństwa informacji. Na

potwierdzenie doświadczenia Wykonawca dołączy do oferty Referencje potwierdzające realizację minimum 2 wystąpień/szkoleń/prelekcji o związanych z tematyką bezpieczeństwa informacji przeprowadzonych w okresie ostatnich 3 lat od złożenia oferty, a jeżeli ten okres jest krótszy to w tym okresie

7. **Materiały szkoleniowe:** Wykonawca zobowiązany jest do przygotowania i dostarczenia uczestnikowi materiałów szkoleniowych w formie drukowanej oraz elektronicznej
8. **Ocena efektywności szkolenia:** Po zakończeniu szkolenia, wykonawca przeprowadzi test wiedzy oraz ankietę ewaluacyjną w celu oceny efektywności szkolenia i zadowolenia uczestnika.
9. **Certyfikat:** Szkolenie powinno zakończyć się certyfikatem imiennym potwierdzającym odbycie się szkolenia

II.1.16. Szkolenie z oprogramowania do zarządzania infrastrukturą IT

1. **Przedmiot zamówienia**: przeprowadzenie specjalistycznego szkolenia dla ASI z wdrożonego oprogramowania do zarządzania infrastrukturą IT – 1 osoba.
2. **Cel szkolenia**: Celem szkolenia jest podniesienie kwalifikacji zawodowych Administratora Systemów Informatycznych (ASI) Urzędu Miasta i Gminy w zakresie zarządzania infrastrukturą IT, w tym zarządzania sieciami komputerowymi, serwerami, bazami danych oraz aplikacjami.
3. **Zakres merytoryczny szkolenia:** Zakres szkolenia musi obejmować minimum:
   a) Wprowadzenie i Kluczowe funkcjonalności i możliwości, Przegląd wersji oprogramowania
   b) Instalacja i konfiguracja oprogramowania, Wymagania systemowe, Wstępna konfiguracja i ustawienia
   c) Moduły oprogramowania: Omówienie poszczególnych modułów: Network, Inventory, Users, HelpDesk, DataGuard, Monitoring, Przykłady zastosowania każdego z modułów w celu uniknięcia cyber zagrożeń,
   d) Szczegółowe omówienie modułu Network z naciskiem na bezpieczeństwo sieci w kontekście monitoringu urządzeń sieciowych
   e) Szczegółowe omówienie modułu Inventory: Automatyczna inwentaryzacja sprzętu i oprogramowania, Raportowanie stanu zasobów
   f) Szczegółowe omówienie modułu Monitorowanie aktywności użytkowników, Zarządzanie kontami użytkowników, Przykłady polityk bezpieczeństwa
   g) Szczegółowe omówienie modułu HelpDesk w tym min. Tworzenie i zarządzanie zgłoszeniami, Konfiguracja portalu HelpDesk, Integracja z innymi modułami
   h) Szczegółowe omówienie modułu Ochrona danych i zarządzanie dostępem
   i) Szczegółowe omówienie modułu Monitoring, Konfiguracja i zarządzanie monitorowaniem, Analiza i interpretacja danych z monitoringu, Automatyzacja zadań monitorowania
   j) Zaawansowana konfiguracja oprogramowanie w kontekście analizy zagrożeń bezpieczeństwa sieci i monitorowania aktywności użytkowników w celu zapobiegania nałażeniom na incydenty: Skrypty i automatyzacja procesów, Personalizacja ustawień i polityk, Audytowanie i raportowanie
4. **Forma i organizacja szkolenia**:
   1) Szkolenie powinno być przeprowadzone w formie warsztatów stacjonarnych, z wykorzystaniem prezentacji multimedialnych, studiów przypadków oraz ćwiczeń praktycznych
   2) Zamawiający oświadcza, że udostępni Wykonawcy miejsce na czas przeprowadzenia szkolenia
5. **Termin realizacji**:
   1. Wykonawca przekaże Zamawiającemu agendę szkolenia wraz z proponowanym terminem przeprowadzenia szkolenia uwzględnionym w Harmonogramie wdrożenia
   2. Przewidywany czas szkolenia – min. 2 dni po 8 godz.
6. **Wymagania wobec wykonawcy:** Wykonawca lub każda wskazana przez Wykonawcę osoba do prowadzenia szkolenia posiada co najmniej 2-letnie doświadczenie zawodowe (praktyczne i/lub dydaktyczne) w zakresie wystąpień/szkoleń/prelekcji o tematyce bezpieczeństwa informacji. Na potwierdzenie doświadczenia Wykonawca dołączy do oferty Referencje potwierdzające realizację minimum 2 wystąpień/szkoleń/prelekcji o związanych z tematyką bezpieczeństwa informacji przeprowadzonych w okresie ostatnich 3 lat od złożenia oferty, a jeżeli ten okres jest krótszy to w tym okresie
7. **Materiały szkoleniowe:** Wykonawca zobowiązany jest do przygotowania i dostarczenia uczestnikowi materiałów szkoleniowych w formie drukowanej oraz elektronicznej
8. **Ocena efektywności szkolenia:** Po zakończeniu szkolenia, wykonawca przeprowadzi test wiedzy oraz ankietę ewaluacyjną w celu oceny efektywności szkolenia i zadowolenia uczestnika.

9. Certyfikat: Szkolenie powinno zakończyć się certyfikatem imiennym potwierdzającym odbycie się szkolenia

II.2 Wymagane minimalne parametry techniczne dla urządzeń i usług ujętych w Części nr 2 zamówienia.

II.2.1 Oprogramowanie do zarządzania infrastrukturą IT na 31 licencji

1. Zamawiający wymaga dostarczenia oprogramowania wraz z licencjami spełniającego poniższe graniczne minimalne parametry techniczne.

Lp.	Przedmiot zamówienia	Minimalne parametry wymagane
1.	Oprogramowanie:	1. Budowa modułowa, 2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. 3. Program umożliwia zmianę portu komunikacyjnego wykorzystywanego przez konsolę zarządzającą. 4. Silnik bazy danych musi być dostępny na licencji open source bez limitu ilości danych 5. Baza danych musi być darmowa i nie wymagać dodatkowego licencjonowania
2.	Monitorowanie danych użytkownika:	1. historia aktywności 2. polityka korzystania z Internetu i aplikacji 3. dostęp do zewnętrznych nośników danych, 4. grupowanie informacji w oddzielnym oknie, co umożliwia usuwanie danych użytkownika zgodne z RODO bez konieczności usunięcia informacji o stacji roboczej, 5. dostęp do danych osobowych oraz danych z monitoringu zgodnie z RODO, 6. możliwość nadawania kontom różnych poziomów dostępu oraz uprawnień do funkcji Programu, grup urządzeń i użytkowników, 7. lista kont użytkowników i administratorów, może być synchronizowana z usługą typu Active Directory, przez szyfrowane połączenia, 8. konfiguracja haseł użytkownika 9. uwierzytelnianie logowań do konsoli z wykorzystaniem weryfikacji dwuskładnikowej
3.	Funkcjonalności:	Oprogramowanie obsługuje min. 6 funkcjonalności: 1. Monitorowanie infrastruktury, 2. Inwentaryzacja sprzętu i oprogramowania, 3. Monitorowanie aktywności użytkowników, 4. Realizacja zdalnej pomocy użytkownikom, 5. Ochrona danych przed wyciekiem, 6. Wsparcie zarządzania czasem i analizowanie aktywności użytkowników
4.	Monitorowanie infrastruktury:	1. Wykrywanie urządzeń w sieci poprzez skanowanie ping oraz arp-ping, 2. Wizualizacja urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki, tworzenie spersonalizowanych map z możliwością zablokowania mapy urządzeń przed przypadkową edycją, 3. Serwisy TCP/IP, HTTP, POP3, SMTP, FTP i inne wraz z możliwością definiowania własnych serwisów. Monitorowanie czasu ich odpowiedzi i procent utraconych pakietów, 4. Serwery pocztowe: - program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty, - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie,

		- program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa 5. Monitorowanie serwerów WWW i adresów URL 6. Cykliczne monitorowanie czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS 7. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail 8. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID 9. Obsługa komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych 10. Monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych - ruchu sieciowego - podłączonych stacji roboczych – graficzna prezentacja panelu switcha - ruchu generowanego przez podłączone do portów stacje robocze 11. Monitor serwisów alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie, zatrzymanie lub zrestartowanie, 12. Wyświetlanie statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu 13. Monitorowanie stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano 14. Zarządzanie stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny 15. Wydajność systemów m.in. obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy, 16. Nakładanie na urządzenia liczników wydajności WMI oraz SNMP z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi, wyłączenie/restart komputera. 17. Administrator samodzielnie może konfigurować zdarzenia, lub wybrać zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. 18. Alarmy muszą pozwalać na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. 19. Oprogramowanie musi umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0
5.	Inwentaryzacja sprzętu i oprogramowania,	1. Automatyczne gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych, min. modelu, procesora, pamięci, płyty głównej, napędów, 2. Umożliwienie odczytów parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe. 3. Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 4. Informacja o zainstalowanych aplikacjach oraz aktualizacjach systemu 5. Zbieranie informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. 6. Możliwość wysyłania powiadomienia np. e-mailem w przypadku jakiejkolwiek zmiany na urządzeniu 7. Możliwość odczytania numeru seryjnego (klucze licencyjne).

		8. Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. 9. Możliwość przeglądania informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. 10. Możliwość utworzenia listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu). 11. Możliwość wymiany plików do i ze stacją roboczą poprzez funkcję Menedżera plików. *Moduł inwentaryzacji zasobów musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:* 12. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, 13. przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów, 14. tworzenia powiązań między zasobami a urządzeniami, 15. tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z funkcjonującą w Urzędzie Active Directory), wskazywanie osób odpowiedzialnych, 16. wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy, 17. definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości, 18. określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, 19. określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, 20. masową edycję atrybutów zasobów, 21. definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, 22. importu danych z zewnętrznego źródła (.CSV), 23. przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., 24. tworzenia powiązań między zasobami a dokumentami w relacji 1:N, 25. oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., 26. ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, 27. generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, 28. przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, 29. konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, 30. konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, 31. archiwizacji i porównywania audytów zasobów, 32. tworzenia kodów kreskowych dla zasobów,

		33. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, 34. inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet, 35. możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android, 36. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), 37. definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data" z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja"). *Inwentaryzacja oprogramowania musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:* 1) Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. 2) Informacje o aplikacjach używanych w organizacji. 3) Tworzenie własnych wzorców aplikacji. 4) Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. 5) Informacje o komputerach, na których aplikacja została wykryta. 6) Zarządzanie posiadanymi licencjami. 7) Wskazywanie osób odpowiedzialnych za licencję. 8) Wskazanie użytkowników licencji, 9) Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. 10) Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
6.	Monitorowanie aktywności użytkowników:	1. Faktyczny czas aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy), 2. Otwarte procesy wraz z informacją o uruchomieniu na podwyższonych uprawnieniach, 3. Rzeczywiste użytkowanie programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność, 4. Informacja o edytowanych przez użytkownika dokumentach, 5. Historia pracy (cykliczne zrzuty ekranowe), 6. Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt), 7. Transfer sieciowy użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), 8. Wydruki m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program powinien mieć możliwość monitorowania kosztów wydruków, 9. Nagłówki przesyłanej w aplikacjach klienckich poczty e-mail.

		10. Wykrywanie podejrzanej aktywności przez popularne „jigglery", mającej na celu symulowanie faktycznej pracy. 11. Zdefiniowanie czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury. 12. Wyszczególnienie podejrzanej aktywności w raportach. 13. Wygenerowanie alarmu i wykonanie akcji po wykryciu podejrzanej aktywności. 14. Automatyczne włączenie zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności. 15. Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). 16. Blokowania ruchu na wskazanych portach TCP/IP, 17. Blokowanie pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem, 18. Prowadzenie rejestru naruszeń blokad, 19. Wysyłanie powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady, 20. Przygotowanie zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika), 21. Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.
7.	Realizacja zdalnej pomocy użytkownikom	1. Dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika, 2. Możliwość równoczesnego podłączenia do tego samego komputera kilku administratorów. 3. Oprogramowanie powinno zawierać komunikator (czat), który umożliwi prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów. Czat powinien pozwalać na: 4. zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej 5. rozmowy między „zwykłymi" użytkownikami 6. przesyłanie plików między rozmówcami w trybie online 7. tworzenie pokojów tematycznych, rozmów grupowych 8. oznaczanie kontaktów jako „ulubionych" na liście kontaktów 9. uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku, 10. Administrator powinien mieć możliwość tworzenia szkiców i archiwizowania komunikatów. Moduł pomocy zdalnej powinien umożliwiać: 11. pobieranie listy użytkowników z Active Directory, 12. wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym, 13. zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,

		14. zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez system zarządzania regułami widoczności zgłoszeń, 15. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń, 16. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy, 17. tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO, 18. automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników, 19. definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji, 20. przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii, 21. procesowanie zgłoszeń użytkowników z wiadomości e-mail, 22. eksportowania listy zgłoszeń do plików CSV i XLSX, 23. integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0, 24. tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń, 25. wykonywanie operacji na wielu zgłoszeniach równocześnie, 26. dołączanie załączników do zgłoszeń, 27. rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, 28. szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, 29. wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia, 30. zrzuty ekranowe (podgląd pulpitu), 31. zdalną modyfikację rejestrów, 32. dystrybucję oprogramowania przez Agenty, 33. dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), 34. możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu, 35. możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy, 36. planowanie nieobecności pracowników helpdesk, 37. obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem, 38. generowanie raportów obsługi helpdesk, 39. zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu), 40. zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), 41. wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.
8.	Ochrona danych przed wyciekiem	Blokowanie urządzeń i nośników danych: 1. możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. 2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. 3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.

		4. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. 5. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender. 6. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker. 7. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker. 8. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu. 9. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu. 10. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender 11. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM. Zarządzanie prawami dostępu do urządzeń: 1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. 2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. 3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników. 4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. 5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane. Audyt operacji na plikach na urządzeniach przenośnych: 1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. 2. Podłączenie/odłączenie urządzenia przenośnego. 3. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. 4. Definiowanie reguł monitorowanych folderów w postaci list. Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.) Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.
9.	Zarządzanie czasem i analizowanie aktywności użytkowników	1. Możliwość oznaczenia sesji aktywności jako czas prywatny gdy pracownik wykonuje czynności prywatne na sprzęcie firmowym. 2. Użytkownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. 3. Zastosowane reguły powinny pozwalać zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. 4. Dostęp powinien być realizowany przez przeglądarkę internetową, a strona powinna być wyświetlana w trybie jasnym lub ciemnym. 5. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. 6. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem. 7. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.

		8. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników. 9. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych. 10. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne. 11. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy. 12. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie). 13. Wskaźnik czasu poświęconego na aktywność produktywną. 14. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail. 15. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Rozrywka - predefiniowana lista kategorii z możliwością edycji. 16. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.
10.	Gwarancja, wsparcie serwisowe	1. Wsparcie techniczne przez min. rok od dnia podpisania protokołu odbioru 2. W ramach wsparcia technicznego możliwość instalowania wszelkich aktualizacji oprogramowania, które zostaną wydane w czasie obowiązywania wsparcia, w tym aktualizacji obejmujących przejście na wyższą wersję oprogramowania. 3. Telefoniczne i mailowe wsparcie techniczne dla oprogramowania 4. Dokonywanie przez Producenta szczegółowej analizy zgłoszonych przypadków (logów). 5. Świadczenie przez Producenta pomocy w formie sesji zdalnych. 6. Czas reakcji na zgłoszenie nie dłuższy niż następny dzień roboczy. 7. Możliwość przedłużenia wsparcia o kolejny rok 8. Możliwość rozszerzenia oprogramowania o dodatkowe licencje i moduły

II.2.2 Usługa zabezpieczenia poczty na 24 miesiące

1. Zamawiający w ramach przedmiotu zamówienia wymaga dostarczenia usługi zabezpieczenia poczty spełniającej poniższe minimalne parametry techniczne:

Lp.	Minimalne parametry wymagane
1.	system ochrony poczty elektronicznej przed wiadomościami niepożądanymi typu spam, wirusy i oprogramowanie złośliwe, phishing, wyłudzenia, podszywanie, manipulacja tożsamością i inne zagrożenia bezpieczeństwa informatycznego.
2.	System filtrujący, portal konfiguracji polityki bezpieczeństwa, system zarządzania i raportowania dostępne jako usługi chmurowe
3.	ochrona przed wiadomościami niepożądanymi za pomocą filtracji poczty przychodzącej i ochronę reputacji własnego systemu pocztowego przez filtrację poczty wychodzącej.
4.	Przekierowanie ruchu pocztowego do chmury obsługiwane na poziomie konfiguracji rekordów Mail Exchange (MX) w systemie DNS.
5.	Chmurowy system ochrony powinien umożliwiać obsługę wielu domen pocztowych jednocześnie (nie mniej niż 15).
6.	Chmurowy system ochrony powinien zapewniać ochronę przed wolumetrycznymi atakami Denial-of-Service
Funkcjonalność filtracji poczty przychodzącej:	

7.	Filtracja wiadomości typu spam:	- wszystkie przychodzące wiadomości powinny być klasyfikowane pod kątem prawdopodobieństwa, że jest to wiadomość typu spam - klasyfikacja powinna być automatyczna i pracować bez ingerencji administratora lub konfiguracji - możliwość zaprogramowania poziomu tolerancji na spam: od całkowitej blokady do całkowitej akceptacji wszystkich wiadomości sklasyfikowanych jako spam - możliwość zaprogramowania typu reakcji na spam: co najmniej „blokada", „kwarantanna", „akceptacja",
8.	Filtracja wiadomości ze względu na kategorię komunikacji:	- oprócz filtrowania wiadomości typu spam system powinien rozpoznawać inne, często niejednoznaczne kategorie komunikacji, co najmniej: komunikację służbową, komunikację handlową, komunikację marketingową, komunikację związaną z listami mailingowymi, komunikację związaną z mediami społecznościowymi, komunikację rozsyłaną masowo - dla każdej rozpoznanej kategorii powinna być możliwość zaprogramowania reakcji, co najmniej: „blokada", „kwarantanna", „akceptacja"
9.	Filtracja wiadomości zawierających wirusy i oprogramowanie złośliwe, zagrożenia ATP i zagrożenia Zero-Day	- możliwość skanowania przez silnik antywirusowy - możliwość skanowania przez silnik sandboxingowy: wykrywanie zagrożeń zamaskowanych typu *Advanced Persistent Threats* (ATP) i zagrożeń typu *Zero-Day* - polityka skanowania ATP powinna umożliwiać konfigurację wyjątków opartych na adresach IP, na adresach nadawców i odbiorców poczty elektronicznej
10.	Filtracja wiadomości phishingowych, wiadomości związanych z wyłudzeniami, ochrona przed złośliwymi adresami URL:	- możliwość filtrowania wiadomości pod kontem phishingu, inżynierii socjalnej, próbami wyłudzeń i kradzieży tożsamości - możliwość filtrowania i ochrony adresów URL zawartych w wiadomościach przed złośliwym wykorzystaniem i zmianą zawartości po dostarczeniu do odbiorcy (*link protection, typosquatting protection*
11.	Filtracja wiadomości na podstawie informacji geograficznych (GeoIP) i językowych	- możliwość blokowania lub umieszczania w kwarantannie poczty przychodzącej z wybranego kraju (np. z Somalii) - możliwość blokowania lub umieszczania w kwarantannie poczty w określonym języku (np. chińskim)
12.	Filtracja wiadomości na podstawie zawartości - możliwość blokowania lub umieszczania w kwarantannie	- wiadomości z załącznikami o określonej nazwie lub o okroślonym typie MIME - wiadomości z załącznikami zaszyfrowanymi, co najmniej: archiwa takie jak ZIP, pliki Microsoft Office, pliki PDF - wiadomości zawierających wskazane słowa kluczowe w nagłowkach, temacie, zawartości lub w załącznikach

13.	Filtracja wiadomości przychodzących na podstawie polityk DNS, SPF, DKIM i DMARC	- możliwość weryfikacji domeny nadawcy: blokowanie nadawców z nieskonfigurowanym rekordem PTR - możliwość weryfikacji nadawcy za pomocą polityki *Sender Policy Framework (SPF)* - możliwość weryfikacji nadawcy za pomocą polityki *Domain Key Identified Email (DKIM)* - możliwość weryfikacji nadawcy za pomocą polityki *Domain Based Message Authentication (DMARC)*
Funkcjonalność związana z kwarantanną i buforowaniem wiadomości:		
14.	Kwarantanna i buforowanie wiadomości	- możliwość pracy z kwarantanną indywidualną, skonfigurowaną i dostępną per użytkownik - możliwość pracy z kwarantanną globalną
15.	Buforowanie i udostępnianie wiadomości w przypadku awarii docelowego serwera pocztowego:	- odbiór i buforowanie wiadomości przychodzących do czasu usunięcia awarii docelowego serwera pocztowego (co najmniej 96 godzin) - udostępnienie zbuforowanych wiadomości użytkownikom za pomocą interfejsu webowego, pozwalającego odczytywać i odpowiadać na wiadomości w czasie awarii - synchronizację wiadomości z serwerem docelowym po usunięciu awarii
16.	Buforowanie wiadomości przychodzących	- system powinien umożliwiać administratorowi przeszukiwanie przychodzących transmisji, co najmniej z ostatnich 30 dni - system powinien umożliwiać zmianę decyzji blokującej wiadomość z ostatnich 30 dni i dostarczenie zablokowanej wiadomości do odbiorcy
Funkcjonalność filtracji poczty wychodzącej:		
17.	skanowanie wiadomości wychodzących:	- wiadomości zawierające wirusy powinny być blokowane - wiadomości podejrzane o spam powinny być blokowane lub poddane kwarantanni
18.	Filtracja wiadomości wychodzących z możliwością kwarantanny:	- filtracja nazw i typów MIME załączonych plików - filtracja zaszyfrowanych i chronionych hasłem plików archiwów, plików Microsoft Office, plików PDF - filtracja na podstawie słów kluczowych w nagłowkach, temacie, zawartości, załącznikach, adresie nadawcy lub adresie odbiorcy
Monitorowanie i raportowanie:		
19.	Możliwość wyświetlania raportów i eksportu raportowanych danych do pliku, co najmniej	- analiza ruchu pocztowego przychodzącego i wychodzącego w zadanym czasie: liczba wiadomości przychodzących, zablokowanych, zablokowanych ze względu na spam, wirusy lub zagrożenia ATP - analiza użytkowników: odbiorcy i nadawcy spamu i wirusów analiza użytkowników: najczęściej blokowani odbiorcy i nadawcy
Funkcjonalność związana z integracją z systemami zewnętrznymi		
20.	Możliwość integracji z zewnętrznym systemem monitorowania	- wsparcie dla protokołu SYSLOG z szyfrowaniem w standardzie TLS

Warunki Gwarancji i serwisu	
21.	Wsparcie techniczne musi zapewniać dostęp do poprawek oprogramowania oraz wsparcia technicznego producenta z czasem reakcji nie dłuższym niż 2 godziny od momentu zgłoszenia problemu
22.	Wymagana jest dostępność usługi w trybie 8x5 w godzinach od 8:00 do 15:00 (e-mail; telefon) 24x7 poprzez zgłoszenie Email.

II.2.3 Usługa zabezpieczenia serwisu www na 24 miesiące:

1. Zamawiający w ramach przedmiotu zamówienia wymaga dostarczenia do Zamawiającego usługi zabezpieczenia serwisu stron internetowych na 24 miesiące spełniającego minimalne parametry techniczne opisane poniżej:

Lp.	Opis przedmiotu zamówienia/ Minimalne parametry wymagane
1.	Dostęp do platformy umożliwiającej ochronę wybranych stron internetowych.
2.	Dostarczona usługa w postaci subskrypcji ważnej 24 miesiące powinna: posiadać funkcje ochrony Web Application Firewall (WAF) i Captcha, - zapewniać zaawansowaną ochronę przed atakami DDoS, - umożliwiać dostęp do globalnej sieć dostarczania treści (CDN), - zapewniać szyfrowanie i optymalizację SSL, - obsługiwać IPv6, - automatycznie buforować treści statyczne, - zapewnić utrzymanie statycznych elementów serwisu online również w przypadku awarii serwera, - zapewnić zabezpieczenie przed kopiowaniem treści, w tym tekstu, obrazów i adresów e-mail przed mechanizmami automatycznie zbierającymi treści z Internetu, - uniemożliwiać dostępu do serwisu z indywidualnych adresów IP, zakresów adresów, lub z określonych krajów.
3.	poprawa wydajności strony internetowej
4.	działa jako autorytatywny serwer DNS, co odpowiada za kierowanie ruchu do strony internetowej.
5.	możliwość samodzielnego zarządzania usługą poprzez panel administracyjny, możliwość skalowania i elastycznego dobierania funkcjonalności,
6.	zapewnienie regionalnego (PL) podstawowego wsparcia technicznego w minimalnym przedziale od poniedziałku do piątku w godzinach min. 08:00 – 15:00.

Rozdział III. Gwarancja

1. Wykonawca w ramach realizacji Przedmiotu Zamówienia udzieli Zamawiającemu gwarancji na poszczególne urządzenia. Zestawienie terminów minimalnej wymaganej gwarancji dla poszczególnych urządzeń przedmiotu zamówienia została uwzględnione w Tabeli nr 3 – Zestawienie gwarancji.

Rozdział	Opis	Minimalny wymagany okres gwarancji [miesiąc]
II.1.1	Serwer I - Dostawa, instalacja i wdrożenie serwerów w celu utworzenia klastra pracy awaryjnej urzędu. Konfiguracja klastra	36
II.1.2	Serwer II - Dostawa serwera	36
II.1.4	Macierz - Dostawa, instalacja, konfiguracja macierzy z klastrem pracy awaryjnej, Przeniesienie danych z dotychczasowych nośników.	60
II.1.8	Przełącznik dystrybucyjny L3	60
II.1.9	Przełączniki sieciowe - Dostawa i wdrożenie zarządzalnych przełączników sieciowych do utworzenia rdzenia sieci LAN	12

II.1.10	IIDostawa, instalacja oraz podłączenie zasilacza awaryjnego UPS z kartą SNMP	24
II.1.11	Dostawa wraz z montażem i uruchomieniem dysków 12TB przeznaczonych do wykonywania kopii zapasowych – 5 szt	36

Tabela nr 3 – Zestawienie Gwarancji

2. Wykonawca zobowiązany jest do udzielenia gwarancji i wparcia technicznego zgodnie z parametrami wymagań technicznych opisanych indywidualnie w rozdziale II.
3. W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu Zamówienia rozumianych jako Awaria lub Błąd lub Usterka zgodnie z definicjami jak poniżej:
   1) **Awaria -** Kategoria Wady w Oprogramowaniu lub Infrastrukturze Sprzętowej powodująca brak działania lub niepoprawne działanie Przedmiotu Zamówienia u Zamawiającego, uniemożliwiające jego użytkowanie. Sytuacja, w której dane rozwiązanie w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcjonalności Komponentów/Produktów Przedmiotu Zamówienia
   2) **Usterka -** Należy przez to rozumieć kategorię Wady w Oprogramowaniu lub Infrastrukturze Sprzętowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz OPZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.
4. Przyjęcie zgłoszenia Wady przez Wykonawcę, odbywać się będzie poprzez dostępny on-line System Zgłaszania i przyjmowania uwag oraz Wad (dalej zwany SZ) przy czym:
   1) System Zgłoszeń dostarczy Wykonawca (będzie on utrzymywany i administrowany przez Wykonawcę), wpis zgłoszenia do SZ będzie dokonywał Zamawiający,
   2) za skuteczne przyjęcie zgłoszenia Wady uważa się będzie wprowadzenie przez Zamawiającego wpisu do SZ zawierającego opis zgłaszanej Wady i termin jej zgłoszenia; w razie trudności z dostępem on-line do SZ, zgłoszenia Wady mogą odbywać się także telefonicznie pod ustalonym numerem telefonu lub pisemnie na formularzu przesyłanym na ustalony adres e-mail, opcjonalnie faksem, których numery i adresy zostaną podane przez Wykonawcę w terminie 15 dni roboczych od dnia podpisania Umowy wraz ze wzorem formularza zgłoszenia Wady.
5. Gwarancja musi zapewniać wymianę uszkodzonego sprzętu, kabli i elementów oraz zapewniać dostęp do aktualizacji oprogramowania, bez wiedzy i wsparcia technicznego producenta.
6. W ramach gwarancji Wykonawca będzie świadczył następujące usługi:
   1) Usuwanie Wad w dostarczonym Przedmiocie Zamówienia w przypadku stwierdzenia przez Zamawiającego Wady w jego działaniu, w terminach określonych poniżej:
   2) dopuszcza się zmianę kwalifikacji zgłoszenia Wady, po uprzedniej zgodzie Zamawiającego. Do czasu potwierdzenia zmiany kwalifikacji, uznaje się za obowiązującą kwalifikację pierwotną,
   3) czasy naprawy mogą być inne niż wskazane w powyższej tabeli, jeżeli Zamawiający zaakceptuje zmianę kwalifikacji zgłoszenia, o której mowa w punkcie 2),
   4) w przypadku braku możliwości usunięcia Wady lub przedstawienia rozwiązania zastępczego zdalnie, Wykonawca zobowiązany jest do świadczenia gwarancji bezpośrednio w lokalizacji Zamawiającego,
   5) Wykonawca w okresie trwania gwarancji, do 5 dnia każdego miesiąca, przedstawi Zamawiającemu raport zawierający co najmniej: numer zgłoszenia, kwalifikację zgłoszenia, godzinę i datę zgłoszenia, temat zgłoszenia, status zgłoszenia, godzinę i datę usunięcia Wady, czas naprawy,

Uwaga:

W przypadku zapisu terminu jako:

- Dzień Roboczy należy rozumieć każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
- Godziny Robocze należy rozumieć godziny od 8.00 do 15.00 w każdym Dniu Roboczym. W innych przypadkach należy rozumieć jako dzień kalendarzowy.

Załącznik nr 2

FORMULARZ OFERTY (wzór)

1…..... …..
Nazwa wykonawcy/wykonawców składających ofertę wspólną Data sporządzenia

2.....
Wykonawca jest/nie jest płatnikiem VAT

3…..
Nr telefonu

4…..
Nr REGON

5.....
Nr NIP

6.…..
e-mail do korespondencji

7…..
Nazwisko i imię osoby/osób uprawnionych
do występowania w imieniu wykonawcy

GMINA MIASTKO
ul. Grunwaldzka 1
77 - 200 Miastko

1. Nawiązując do opublikowanego w Biuletynie Zamówień Publicznych (platforma https://ezamowienia.gov.pl) ogłoszenia Nr …..... z dnia …..... …..... 2024 r. o postępowaniu ws. udzielenia zamówienia publicznego na usługę, prowadzonego w trybie podstawowym, na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2024 r., poz. 1320) o wartości zamówienia mniejszej niż progi unijne określone w przepisach wydanych na podstawie art. 3 ust. 3 przywołanej ustawy, na wykonanie zamówienia **„ Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko.”** i po zapoznaniu się z warunkami prowadzonego postępowania :
   1) **Część I - rozbudowa infrastruktury informatycznej urzędu opartą na dostawie sprzętu wraz z instalacją, montażem i przeniesieniem danych z obecnej sieci informatycznej oraz wdrożenie oprogramowania do zarządzania siecią IT wraz z konfiguracją sieci VLAN.**
   a) Oferujemy i zobowiązujemy się do wykonania zamówienia:
      Za cenę ryczałtową w kwocie brutto….....…….…….....PLN
      (wraz z podatkiem VAT),
      (słownie ….....),
      w tym:
      cena netto ……..PLN
      (słownie:…….……..……),

podatek VAT …….PLN,
(słownie: ……..…..……),
wg obowiązującej stawki w wysokości …..……..%.
obejmującą:

LP.	Rodzaj zamawianego asortymentu	Ilość sztuk/kpl	Cena netto	VAT	Cena brutto
1.	Serwer I - Dostawa, instalacja i wdrożenie serwerów w celu utworzenia klastra pracy awaryjnej urzędu. Konfiguracja klastra	3 szt.			
2.	Serwer II - Dostawa serwera	1 szt.			
3.	Oprogramowanie i licencje do serwerów				
	Oprogramowanie	8 szt.			
	Bezterminowa licencja dostępowa na użytkownika	110			
	Bezterminowa licencja dostępowa na urządzenie	30			
4.	Macierz - Dostawa, instalacja, konfiguracja macierzy z klastrem pracy awaryjnej, Przeniesienie danych z dotychczasowych nośników.	1 szt.			
5.	Dostawa i wdrożenie oprogramowania do wykonywania kopii zapasowych wraz z usługą chmurową	1 szt.			
6.	Wdrożenie oprogramowania do zarządzania infrastrukturą IT na 80 licencji	1 szt.			
7.	Wdrożenie usług domeny do zarzadzania siecią i zasobami komputerowymi	1 szt.			
8.	Przełącznik dystrybucyjny L3	1 szt.			
9.	Przełączniki sieciowe - Dostawa i wdrożenie zarządzalnych przełączników sieciowych do utworzenia rdzenia sieci LAN	6 szt.			
10.	Dostawa, instalacja oraz podłączenie zasilacza awaryjnego UPS z kartą SNMP	1 szt.			
11.	Dostawa wraz z montażem i uruchomieniem dysków 12TB przeznaczonych do wykonywania kopii zapasowych	5 szt.			
12.	Szkolenie ASI tworzenie i administracja sieci VLAN	1 szt.			
13.	Szkolenie ASI tworzenie i administracja serwerami Windows	1 szt.			
14.	Szkolenie ASI z domeny do zarzadzania siecią i zasobami komputerowymi	1 szt.			
15.	Szkolenie ASI Budowa klastra Hyper-V	1 szt.			
16.	Szkolenie z oprogramowania do zarządzania infrastrukturą IT	1 szt.			

UWAGA!

Zamawiający wymaga załączenia do Formularza ofertowego wykazu oferowanego sprzętu wraz ze szczegółowym opisem technicznym znajdującego się w Załączniku nr 2a - Wykaz oferowanego sprzętu wraz z szczegółowym opisem technicznym - w taki sposób aby Zamawiający mógł jednoznacznie określić szczególne cechy produktu oraz wymagane prawem certyfikaty, deklaracje zgodności CE, instrukcje obsługi sprzętu, dokumenty gwarancyjne, celem sprawdzenia zgodności oferowanego produktu.

b) Termin realizacji zamówienia **……. dni kalendarzowych od dnia** (*uzupełnia Wykonawca/termin nieprzekraczalny – nie krótszy 80 dni, nie dłuższy niż 90 dni kalendarzowych*) ;

2) Cz. II - dostawa oprogramowania do monitorowania infrastrukturą sieci informatycznej i urządzeń dla jednostki podległej oraz dostawa usług chmurowych w ramach zabezpieczenia poczty i stron internetowych Gminy.

a) Oferujemy i zobowiązujemy się do wykonania zamówienia:
Za cenę ryczałtową w kwocie brutto….....…….…….....PLN (wraz z podatkiem VAT),
(słownie ….....),
w tym:
cena netto ……..PLN
(słownie:…….…….…….),
podatek VAT …….PLN,
(słownie: ……..……),
wg obowiązującej stawki w wysokości …..…..…..%.
obejmującą:

	Opis	**Ilość sztuk/ kpl**	**Cena netto**	**VAT**	**Cena brutto**
Lp.	**Rodzaj zamawianego asortymentu**				
1.	Oprogramowanie do zarządzania infrastrukturą IT na 31 licencji dla MOPS	1 szt.			
2.	Usługa zabezpieczenia poczty	1 szt.			
3.	Usługa zabezpieczenia serwisu www na 24 miesiące	1 szt.			

<u>UWAGA!</u>

Zamawiający wymaga załączenia do Formularza ofertowego wykazu oferowanego oprogramowania wraz ze szczegółowym opisem technicznym znajdującego się w Załączniku nr 2b- Wykaz oferowanego oprogramowania wraz z szczegółowym opisem technicznym- w taki sposób aby Zamawiający mógł jednoznacznie określić <u>szczególne cechy produktu oraz wymagane prawem certyfikaty, deklaracje zgodności CE, instrukcje obsługi sprzętu, dokumenty gwarancyjne, celem sprawdzenia zgodności oferowanego produktu.</u>

Termin realizacji zamówienia **……. dni kalendarzowych od dnia** (*uzupełnia Wykonawca/termin nieprzekraczalny – nie krótszy niż 20 dni, nie dłuższy niż 30 dni kalendarzowych*) ;

2. Oświadczamy, że:
   1) zapoznaliśmy się z SWZ i nie wnosimy do niej żadnych zastrzeżeń, warunki w niej zawarte akceptujemy bez uwag, zdobyliśmy konieczne informacje do przygotowania oferty;
   2) oferowana przez nas cena wykazana w poz. 1 niniejszej oferty obejmuje wszystkie nakłady określone w SWZ i konieczne do wykonania kompletnego dzieła zgodnie z warunkami prowadzonego postępowania oraz przekazania go do użytkowania;
   3) uważamy się za związanych niniejszą ofertą przez okres wskazany w swz,
      Następujący zakres (cześć) zamówienia powierzymy podwykonawcy/om:
      …….
      ……
   4) Oświadczamy, że w przypadku ujawnienia wad, błędów w wykonanym przedmiocie zamówienia zobowiązujemy się do ich usunięcia na Nasz koszt.

5) Zobowiązujemy się, w przypadku przyznania nam zamówienia, do zawarcia umowy w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty z zastrzeżeniem art. 578 Pzp~~,~~
6) Zobowiązujemy się, w przypadku przyznania nam zamówienia, do zawarcia umowy w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty z zastrzeżeniem art. 578 Pzp;
7) wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[1)] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

3. Wykonawca jest (zaznaczyć właściwą opcję)[*] :

☐ mikroprzedsiębiorstwem

☐ małym przedsiębiorstwem

☐ średnim przedsiębiorstwem

*

Mikroprzedsiębiorstwo:	przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EURO.
Małe przedsiębiorstwo:	przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EURO.
Średnie przedsiębiorstwo:	przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami i które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 milionów EUR lub roczna suma bilansowa nie przekracza 43 milionów EURO.

4. Załącznikami do oferty są:

….....
….....

Oferta zawiera …..... ponumerowanych stron.

…..... ……

Miejscowość i data

Podpis wykonawcy/osoby upoważnionej
do występowania w imieniu wykonawcy

Załącznik 2a

Wykaz oferowanego sprzętu wraz z szczegółowym opisem technicznym

Cz.I - rozbudowa infrastruktury informatycznej urzędu opartą na dostawie sprzętu wraz z instalacją, montażem i przeniesieniem danych z obecnej sieci informatycznej oraz wdrożenie oprogramowania do zarządzania siecią IT wraz z konfiguracją sieci VLAN.

UWAGA!

Zamawiający wymaga dołączenia wykazu oferowanego sprzętu do formularza ofertowego. W pozycji parametry oferowane należy umieścić opis techniczny umożliwiający Zamawiającemu jednoznaczne określenie szczególnych cech produktu oraz wymagane prawem certyfikaty, deklaracje zgodności CE, instrukcje obsługi sprzętu, dokumenty gwarancyjne, celem sprawdzenia zgodności oferowanego produktu.

W przypadku nie dołączenia wymienionego powyżej wykazu do formularza oferty oferta podlega odrzuceniu jako niezgodna z zapisami swz.

1. Dostawa, instalacja i wdrożenie klastra pracy awaryjnej urzędu składającego się z 3 serwerów wraz z systemem operacyjnym.

Zaoferowane serwery musza spełniać minimalne parametry techniczne:

Lp.	Przedmiot zamówienia	Minimalne parametry wymagane	Parametry oferowane
1.	**Obudowa**	Do szafy Rack 19", wysokość 1U, z zestawem szyn do mocowania w szafie;	
2.	**CPU**	Zainstalowane 2 procesory w architekturze x86, dokładnie 8-rdzeniowe, o TDP nie większym niż 165W. Wynik wydajności procesora instalowanego w oferowanym serwerze wynoszący min. 178 punktów w teście SPECrate®2017_int_base, dla konfiguracji dwuprocesorowej. Wynik testu przeprowadzony dla oferowanego modelu serwera oraz zgodnego modelu procesora dostępny na stronie https://www.spec.org/;	
3.	**Płyta główna**	- Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera; - Z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje; - Wyposażona w moduł zabezpieczeń zgodny z TPM 2.0; - Posiadająca 32 sloty DIMM na pamięć DDR5, obsługująca do 8TB pamięci RAM;	
4.	**Pamięć RAM**	- Zainstalowane minimum 128GB pamięci RAM, pracującej w oferowanej konfiguracji z częstotliwością min. 4800MHz, w modułach o pojemności 32GB każdy;	
5.	**Protekcja pamięci RAM**	- Memory mirroring, ECC, Advanced ECC lub SDDC;	
6.	**GPU**	- Wbudowana karta graficzna osiągająca rozdzielczość 1920x1200 przy 60 Hz;	
7.	**Zatoki dyskowe**	- Serwer wyposażony w 8 zatok dyskowych hot-plug 2.5" umożlwiających instalację dysków SSD/HDD z interfejsem SATA/SAS; - Serwer wyposażony w kontroler sprzętowy RAID pozwalający na obsługę RAID 0,1,10,5;	

		- Serwer umożlwiający rozbudowę o 2 dyski M.2 SSD NVMe o pojemności min. 960GB działające ze sprzętowym RAID 1;	
8.	**Zasilanie**	- Dwa zasilacze o mocy min. 1000W z certyfikatem Titanium.	
9.	**Karty sieciowe**	- Karta Ethernet posiadająca 2 porty 10 GbE BASE-T (RJ-45) - Karta Ethernet posiadająca 2 porty 10/25GBE SFP28	
10.	**Sloty PCIe**	- Serwer posiadający 2 sloty PCIe generacji 4.0 dostępne do instalacji kart rozszerzeń bez konieczność rekonfiguracji serwera; - Możliwość rozbudowy oferowanego serwera o 2 karty GPU o pamięci podręcznej min. 16GB oraz wydajności 9 TFLOPS dla obliczeń Tensor-Float 32 każda.	
11.	**Dodatkowe porty**	- z przodu obudowy: 1x USB 3.0, 1x USB 2.0, 1x VGA - z tyłu obudowy: 3x USB 3.0, 1x VGA - wewnętrzne: 1 x USB 3.0	
12.	**Chłodzenie**	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1	
13.	**Zarządzanie**	Serwer wyposażony w moduł zarządzający posiadający dedykowany port 1GbE Base-T Ethernet, pozwalający na zdalny dostęp i zarządzanie serwerem przy użyciu graficznego interfejsu Web. Moduł umożliwia: - monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe - dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub - dostęp do karty możliwy: • z poziomu przeglądarki webowej (GUI) • z poziomu linii komend (SSH lub IPMI) - wbudowane narzędzia diagnostyczne - zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego - obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie - wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników - przesyłanie alertów poprzez e-mail oraz SNMP	

		- obsługa zdalnego serwera logowania (remote syslog) - wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów - monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji - konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) - zdalna aktualizacja oprogramowania (firmware) - możliwość równoczesnej obsługi przez min. 2 administratorów - wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) - możliwość instalacji karty Micro SD udostępniającej min. 4GB przestrzeni na potrzeby karty zarządzającej - Możliwość zarządzania – monitoring parametrów pracy i konfiguracja najważniejszych komponentów - z poziomu urządzania mobilnego przy użyciu dedykowanej aplikacji dostępnej na Android i/lub iOS - Możliwość monitorowania i zarządzania grupą do 200 serwerów z poziomu kontrolera zarządzania pojedynczego serwera Serwer wyposażony w wbudowany panel LCD umieszczony na froncie obudowy i pozwalający na wyświetlenie informacji o: stanie serwera, konfiguracji sieciowej karty zarządzającej, zasilaniu, temperaturze. Możliwość zarządzania – monitoring parametrów pracy i konfiguracja najważniejszych komponentów - z poziomu urządzania mobilnego przy użyciu dedykowanej aplikacji dostępnej na Android i/lub iOS. Oprogramowanie diagnostyczne producenta serwera (lub wbudowana funkcja karty zarządzającej) posiadające funkcjonalność predykcji awarii wszystkich kluczowych komponentów serwera: procesorów, pamięci RAM, dysków wewnętrznych HDD/SSD/M.2 SSD, wentylatorów, zasilaczy, kontrolerów dyskowych.	
14.	**Funkcje zabezpieczeń**	- Czujnik otwarcia obudowy; - TPM 2.0;	
15.	**Urządzenia hot- swap**	Dyski twarde, zasilacze, wentylatory.	

16.	**Gwarancja**	- 36 miesięcy wsparcia technicznego realizowanego w trybie on-site (naprawa na w miejscu instalacji) lub poprzez wysyłkę części; - Usługa wsparcia technicznego świadczona przez producenta lub autoryzowany serwis producenta oferowanych urządzeń;	
17.	**Inne**	- Serwer wyprodukowany zgodnie z normą ISO-9001 oraz ISO14001; - Elementy, z których zbudowane są serwery są produktami producenta tych serwerów lub są przez niego certyfikowane oraz są objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA; - Możliwość rozbudowy serwerów zgodnie z ww. wyżej specyfikacją możliwa przy użyciu dedykowanych dla danego modelu serwera komponentów oraz zachowaniu pełnego wsparcia i gwarancji producenta serwera; - Serwer fabrycznie nowy z oficjalnego kanału dystrybucyjnego w Polsce; - Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanych serwerów, nawet po wygaśnięciu 3-letniego okresu wsparcia	

2. Serwer II - Dostawa serwera

Lp.	Przedmiot zamówienia	Minimalne parametry wymagane	Parametry oferowane
1.	**Obudowa**	- Do szafy Rack 19", wysokość 1U, z zestawem szyn do mocowania w szafie;	
2.	**CPU**	- Zainstalowany 1 procesor w architekturze x86, 16-rdzeniowy, o TDP nie większym niż 150W. Wynik wydajności procesora instalowanego w oferowanym serwerze wynoszący min. 267 punktów w teście SPECrate®2017_int_base, dla konfiguracji dwuprocesorowej. Wynik testu przeprowadzony dla oferowanego modelu serwera oraz zgodnego modelu procesora dostępny na stronie https://www.spec.org/; - Możliwość rozbudowy serwera o drugi procesor tego samego typu co zainstalowany;	
3.	**Płyta główna**	- Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera; - Z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje; - Wyposażona w moduł zabezpieczeń zgodny z TPM 2.0; - Posiadająca 32 sloty DIMM na pamięć DDR5, obsługująca do 8TB pamięci RAM;	
4.	**Pamięć RAM**	- Zainstalowane minimum 64GB pamięci RAM, pracującej w oferowanej konfiguracji z częstotliwością min. 4400MHz, w modułach o pojemności 32GB każdy;	

5.	**Protekcja pamięci RAM**	- Memory mirroring, ECC, Advanced ECC lub SDDC;	
6.	**GPU**	- Wbudowana karta graficzna osiągająca rozdzielczość 1920x1200 przy 60 Hz;	
7.	**Zatoki dyskowe**	- Serwer wyposażony w 4 zatoki dyskowych hot-plug 3.5" umożlwiające instalację dysków SSD/HDD z interfejsem SATA/SAS; - Serwer wyposażony w kontroler sprzętowy RAID pozwalający na obsługę RAID 0,1,10,5; - Serwer umożlwiający rozbudowę o 2 dyski M.2 SSD NVMe o pojemności min. 960GB działające ze sprzętowym RAID 1;	
8.	**Nośniki danych**	- Serwer wyposażony w 2 dyski SSD hot-plug, dedykowane do serwerów, o pojemności 960GB każdy;	
9.	**Zasilanie**	- Dwa zasilacze o mocy min. 1000W z certyfikatem Titanium.	
10.	**Karty sieciowe**	- Karta Ethernet posiadająca 2 porty 10 GbE BASE-T (RJ-45)	
11.	**Sloty PCIe**	- Serwer posiadający 1 sloty PCIe generacji 4.0 dostępny do instalacji kart rozszerzeń bez konieczność rekonfiguracji serwera;	
12.	**Dodatkowe porty**	- z przodu obudowy: 1x USB 3.0 - z tyłu obudowy: 3x USB 3.0, 1x VGA - wewnętrzne: 1 x USB 3.0	
13.	**Chłodzenie**	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1	
14.	**Zarządzanie**	Serwer wyposażony w moduł zarządzający posiadający dedykowany port 1GbE Base-T Ethernet, pozwalający na zdalny dostęp i zarządzanie serwerem przy użyciu graficznego interfejsu Web. Moduł umożliwia: - monitorowanie podzespołów serwera: temperatura, zasilacze, - wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe - dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub - dostęp do karty możliwy: • z poziomu przeglądarki webowej (GUI) • z poziomu linii komend (SSH lub IPMI) - wbudowane narzędzia diagnostyczne - zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego - obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie - wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym	

		włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników - przesyłanie alertów poprzez e-mail oraz SNMP - obsługa zdalnego serwera logowania (remote syslog) - wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów - monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji - konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) - zdalna aktualizacja oprogramowania (firmware) - możliwość równoczesnej obsługi przez min. 2 administratorów - wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) - możliwość instalacji karty Micro SD udostępniającej min. 4GB przestrzeni na potrzeby karty zarządzającej - Możliwość zarządzania – monitoring parametrów pracy i konfiguracja najważniejszych komponentów - z poziomu urządzania mobilnego przy użyciu dedykowanej aplikacji dostępnej na Android i/lub iOS - Możliwość monitorowania i zarządzania grupą do 200 serwerów z poziomu kontrolera zarządzania pojedynczego serwera Możliwość zarządzania – monitoring parametrów pracy i konfiguracja najważniejszych komponentów - z poziomu urządzania mobilnego przy użyciu dedykowanej aplikacji dostępnej na Android i/lub iOS. Oprogramowanie diagnostyczne producenta serwera (lub wbudowana funkcja karty zarządzającej) posiadające funkcjonalność predykcji awarii wszystkich kluczowych komponentów serwera: procesorów, pamięci RAM, dysków wewnętrznych HDD/SSD/M.2 SSD, wentylatorów, zasilaczy, kontrolerów dyskowych.	
15.	**Funkcje zabezpieczeń**	TPM 2.0;	
16.	**Urządzenia hot-swap**	Dyski twarde, zasilacze, wentylatory.	
17.	**Gwarancja**	- 36 miesięcy wsparcia technicznego realizowanego w trybie on-site (naprawa na w miejscu instalacji) lub poprzez wysyłkę części; - Usługa wsparcia technicznego świadczona przez producenta lub autoryzowany serwis producenta oferowanych urządzeń;	

18.	**Inne**	- Serwer wyprodukowany zgodnie z normą ISO-9001 oraz ISO14001; - Elementy, z których zbudowane są serwery są produktami producenta tych serwerów lub są przez niego certyfikowane oraz są objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA; - Możliwość rozbudowy serwerów zgodnie z ww. wyżej specyfikacją możliwa przy użyciu dedykowanych dla danego modelu serwera komponentów oraz zachowaniu pełnego wsparcia i gwarancji producenta serwera; - Serwer fabrycznie nowy z oficjalnego kanału dystrybucyjnego w Polsce; - Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanych serwerów, nawet po wygaśnięciu 3-letniego okresu wsparcia	

3. Oprogramowanie i licencje do serwerów;

Wymagane jest dostarczenie i wgranie oprogramowania oraz licencji na dostarczonych w ramach postępowania serwerach.

Oprogramowanie dla serwerów oraz licencje muszą spełniać poniższe minimalne parametry:

Opis	**Minimalne parametry wymagane**	**Parametr oferowany**
Oprogramowanie – 8 szt.	- System operacyjny dedykowany do serwerów w wersji komercyjnej o zamkniętym kodzie źródłowym. - System operacyjny powinien być dostarczony w najnowszej dostępnej wersji od producenta. - System operacyjny nowy, dostarczony ze wszystkimi atrybutami legalności. - Licencja musi mieć możliwość przenoszenia na inne serwery fizyczne. - Licencja nieograniczona czasowo ani funkcjonalnie. - Licencja wieczysta dla oferowanej konfiguracji serwerów.	
Bezterminowa licencja dostępowa na użytkownika – 110 licencji	- Dostarczona licencja musi być fabrycznie nowa. - Licencja musi być najnowszą wersją, możliwą do nabycia od producenta. - Licencja nieograniczona czasowo ani funkcjonalnie. - Dostarczona licencja musi posiadać cechy/atrybuty legalności.	
Bezterminowa licencja dostępowa na urządzenie – 30 licencji,	- Dostarczona licencja musi być fabrycznie nowa. - Licencja musi być najnowszą wersją, możliwą do nabycia od producenta. - Licencja nieograniczona czasowo ani funkcjonalnie. - Dostarczona licencja musi posiadać cechy/atrybuty legalności.	

4. Macierz - Dostawa, instalacja, konfiguracja macierzy z klastrem pracy awaryjnej, Przeniesienie danych z dotychczasowych nośników. – 1 szt.

Dostarczona macierz powinna spełniać minimalne parametry techniczne:

Lp.	**Przedmiot zamówienia**	**Opis przedmiotu zamówienia/ parametry wymagane**	**Parametr oferowany**
1.	Obudowa	instalacja w szafie technicznej typu RACK 19", Wysokość max. 2U.	

2.	Kontrolery dyskowe	- Min. 2 kontrolery macierzowe pracujące w trybie Symmetrical Active-Active/Mesh Active-Active, to znaczy w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek (path) i portów kontrolerów w trybie bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing) nawet dla pojedynczego LUN. Dla utworzonego jednego LUN operacje I/O muszą być realizowane jednocześnie przez porty w obu kontrolerach, a generowane obciążenie (IOPS oraz Bandwidth) mają być rozłożone dla pary kontrolerów w stosunku 50/50 +/- 10%. - W przypadku zaoferowania większej ilości kontrolerów obciążenie ma być rozłożone proporcjonalnie na wszystkie kontrolery. Kontrolery muszą pozwalać na udostępnianie zasobów protokołami plikowymi oraz blokowymi. Komunikacja pomiędzy oferowanymi kontrolerami macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia; nie dopuszcza się w szczególności komunikacji z wykorzystaniem urządzeń aktywnych FC/Ethernet/Infiniband. Zamawiający dopuszcza komunikację z wykorzystaniem urządzeń aktywnych przy klastrze więcej niż 2 kontrolerów. Każdy z kontrolerów musi mieć możliwość jednoczesnej prezentacji (aktywny dostęp odczyt i zapis) wszystkich wolumenów utworzonych w logicznych ramach całego systemu dyskowego.	
3.	Możliwość rozbudowy	Urządzenie musi umożliwiać podniesienie wydajności i niezawodności poprzez rozbudowę do 6 par kontrolerów, tworzących jedną logiczną macierz dyskową. Rozbudowa musi być możliwa bez konieczności wymiany zaoferowanej pary kontrolerów na nowe. Za jedną logiczną macierz uznaje się rozwiązanie, w którym zarządzanie wszystkimi kontrolerami jest możliwe z jednego interfejsu GUI, CLI. Nie dopuszcza się rozwiązań opartych o wirtualizator. Macierz wyłącznie do obsługi modułów pamięci NVME i w żadnej konfiguracji nie może obsługiwać przestrzeni danych użytkownika na dyskach obrotowych/talerzowych. Urządzenie musi umożliwiać dynamiczną zmianę rozmiaru woluminów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się w danym LUN. Urządzenie musi umożliwiać rozbudowę przestrzeni dyskowej o pojedynczy dysk oraz pojedynczą półkę dyskową z możliwością rozszerzenia puli dyskowej o dodany dysk/półkę bez konieczności migracji danych ani zatrzymywania pracy macierzy.	
4.	Wymagana przestrzeń	Całkowita pojemność surowa RAW urządzenia musi wynosić minimum 23 TB i być zbudowana tylko i wyłącznie za pomocą dysków SSD NVMe/modułów NVMe o maksymalnej pojemności pojedynczego modułu 4 TB.	

		Macierz musi umożliwiać rozbudowę do co najmniej 100 sztuk oferowanego typu modułów pamięci NVMe, bez wymiany lub dodawania kontrolerów macierzowych oraz bez potrzeby zakupu dodatkowych licencji. (tylko poprzez dodawanie półek dyskowych oraz kart z interfejsami i modułów NVMe). Moduły NVMe muszą posiadać redundantne interfejsy PCIe Gen 4.	
5.	Procesory/Pamięć Cache	Każdy kontroler macierzy musi być oparty o wielordzeniowe procesory, minimum dwadzieścia rdzeni łącznie na kontroler. Urządzenie zbudowane z dwóch kontrolerów musi być wyposażone w co najmniej 128 GB pamięci podręcznej cache obsługującej operacje odczytu i zapisu zbudowane w oparciu o wydajną pamięć RAM. Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin.	
6.	Zabezpieczenie danych	Możliwość definiowania dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej. Urządzenie musi obsługiwać poziomy RAID5, RAID6 lub RAID DP (RAID z dystrybuowaną przestrzenią zapasową typu hot-spare), oraz RAID 10.	
7.	Dostępne interfejsy	Macierz musi posiadać: - minimum 8 portów 25 Gb/s lub 4 porty 100GB/s obsługujących protokół NVMe over RoCE. Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+/SFP28,QSFP28), wymaga się ich dostarczenia wraz z urządzeniem; - minimum 2 wkładki jednomodowe ze złączem LC oraz komplet patchcordów jednomodowych o długości 50cm - minimum 8 portów 10Gb/s na całą macierz. Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+/SFP28), wymaga się ich dostarczenia wraz z urządzeniem; - minimum 8 wkładek multimodowych 10Gb/s ze złączem LC oraz komplet patchcordów multimodowych o długości 50cm W oferowanej konfiguracji portów macierz musi posiadać pełną możliwość rozbudowy do wymaganej ilości modułów pamięci bez usuwania żadnego z interfejsów.	
8.	Brak pojedynczego punktu awarii	Wszystkie krytyczne komponenty takie jak adaptery HBA, kontrolery dyskowe, pamięć, zasilacze i wentylatory muszą być zaprojektowane nadmiarowo: tak, aby awaria pojedynczego elementu nie wpływała na ciągłość dostępu do danych całego systemu. Komponenty te muszą być wymienialne w trakcie pracy.	
9.	Prezentacja dysków logicznych o pojemności większej niż zajmowana przestrzeń dyskowa (Thin Provisioning)	Wymagana jest funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation).	

		Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem.	
10.	Protokoły dostępu do danych	Wymagane wsparcie dla NVMe over RoCE, iSCSI, NFS, CIFS. Wymagana obsługa protokołów plikowych minimum: - CIFS (minimum SMB 2.0, SMB 2.1, SMB 3.0, oraz SMB 3.1.1) - NFS (minimum NFSv3, NFSv4.0 oraz NFSv4.1). Dla zasobów udostępnianych plikowo macierz musi posiadać funkcjonalność definiowania polityk umożliwiających limitowanie ilości plików w danym katalogu oraz jego maksymalnego rozmiaru. Nie dopuszcza się realizacji funkcjonalności dostępu plikowego za pomocą dodatkowych/zewnętrznych urządzeń. Funkcjonalność ta musi być wbudowana w oprogramowanie zainstalowane w kontrolerach urządzenia. Dla zasobów plikowych macierz musi posiadać możliwość uruchomienia replikacji w trybach synchronicznym oraz asynchronicznym. Jeśli obsługa protokołów plikowych wymaga dodatkowej licencji, to nie jest wymagane jej dostarczenie wraz z urządzeniem.	
11.	WORM	Dla zasobów plikowych macierz musi umożliwiać skonfigurowanie funkcji Write Once Read Many (WORM) dla utworzonego systemu plików. Każdy plik objęty ochroną WORM musi przechodzić w stan tylko do odczytu natychmiast po zapisaniu na macierzy. W stanie tylko do odczytu plik można odczytać, ale nie można go usunąć, zmodyfikować ani zmienić jego nazwy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie nie jest wymagane wraz z urządzeniem.	
12.	Snapshoty	Urządzenie musi umożliwiać utworzenie 1000 kopii migawkowych (ang. snapshot) w trybie ROW (ang. Redirect on Write) dla pojedynczego wolumenu oraz minimum 4000 dla całej macierzy. Niedopuszczalne jest wykonywanie kopii w technologii COW (ang. Copy-on-Write). Rozwiązanie musi umożliwiać tworzenie grup spójności, które gwarantują spójne kopiowanie, odtwarzanie i odświeżanie wielu wolumenów naraz tj. tworzenie kopii zapasowej wielu LUNów jednocześnie. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem. Rozwiązanie musi umożliwiać hierarchiczne tworzenie kopii migawkowych (np. kopia z kopii z kopii). Dla zasobów plikowych macierz musi umożliwiać wykonywanie kopii migawkowych systemu plików z którego dane udostępniane są protokołem CIFS. Po wykonaniu kopii zmiany danych lub zapisy w systemie plików nie będą miały wpływu na dane kopii migawkowej. Musi istnieć możliwość zabezpieczenia kopii przed modyfikacją i usunięciem przez zadany okres czasu.	
13.	Funkcje kopiujące	Tworzenie na żądanie pełnej kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać	

		synchronizację danych z woluminu źródłowego na docelowy oraz resynchronizację danych z woluminu docelowego na źródłowy np. w sytuacji uszkodzenia danych na woluminie źródłowym. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem.	
14.	Redukcja danych	Macierz musi mieć funkcjonalność deduplikacji i kompresji danych w trybie in-line zarówno dla danych blokowych jak i systemu plików. Administrator musi mieć możliwość wyłączenia mechanizmów redukcji danych dla poszczególnych woluminów LUN. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem.	
15.	Replikacja danych	Macierz musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych z innymi macierzami (ten sam model/rodzina modeli) - w trybie synchronicznym i asynchronicznym - po protokołach NVMe over RoCE lub IP bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji, główek typu serwer/wirtualizator, itp. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem.	
16.	Klaster wysokiej dostępności	Model oferowanej macierzy musi wspierać rozwiązanie klastra „wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów danych macierzy dla podłączonych platform software'owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po NVMe over RoCE lub IP pomiędzy 2 macierzami dostarczonymi w tym postępowaniu. Pod użytym pojęciem „wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie „wysokiej dostępności", musi wspierać klastrowanie wybranych woluminów bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną. Musi być możliwość dodawania woluminów objętych zabezpieczeniem w klastrze bez konieczności zatrzymywania replikacji. Funkcjonalność „wysokiej dostępności" musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover). Funkcjonalność „wysokiej dostępności" musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover). Funkcjonalność „wysokiej dostępności" musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback). Funkcjonalność „wysokiej dostępności" musi wspierać konfiguracje z macierzą zapasową zainstalowaną w	

		innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem.	
17.	Priorytety zadań	Macierz musi posiadać funkcjonalność zarządzania wydajnością, która dynamicznie przydziela zasoby macierzy w celu spełnienia określonych celów wydajnościowych aplikacji (QoS). Możliwość ustawiania priorytetów wydajności dla aplikacji w oparciu o zdefiniowane profile wolumenowe, dla wydajności w IOPS i przepustowości danych. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem.	
18.	Kompatybilność	Model oferowanej macierzy musi znajdować się na oficjalnej liście zgodności VMware (dostępnej na stronie https://www.vmware.com/resources/compatibility/search.php). Rozwiązanie musi wspierać integrację w zakresie technologii konteneryzacji poprzez posiadanie dedykowanego sterownika Container Storage Interface (CSI).	
19.	Licencje	Macierz musi być dostarczona z licencjami wymaganymi do instalacji kontrolerów z dyskami, oraz uruchomienia mechanizmów wymaganych w OPZ.	
20.	Wielościeżkowość	Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: Windows Server 2019 oraz 2022, Vmware 8.0 i nowszych.	
21.	Zasilanie	Urządzenie musi cechować wsparcie dla zasilania z dwóch niezależnych źródeł prądu jednofazowego o napięciu 200-240V i częstotliwości 50-60Hz poprzez nadmiarowe zasilacze typu Hot-Swap.	
22.	Zarządzanie macierzą	Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy (w tym monitorowanie wydajności) oraz możliwość konfigurowania jej zasobów. Wymagana możliwość monitorowania stanu żywotności modułów NVME. Konsola graficzna musi być dostępna poprzez przeglądarkę internetową i być elementem systemu operacyjnego macierzy. Wymaga możliwość dostępu do danych wydajnościowych historycznych z poziomu GUI z co najmniej 2 lat wstecz. Macierz musi umożliwiać monitorowanie oraz przeglądanie danych historycznych z podziałem dla każdego z LUN dla min. operacji: -% trafień w cache do odczytu oraz zapisu -IOPS -średni czas odpowiedzi dla odczytu danych -średni czas odpowiedzi dla zapisu danych -przepustowość „Bandwidth" dla operacji odczytu -przepustowość „Bandwidth" dla operacji zapisu Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.	

		Rozwiązanie musi udostępniać interfejs REST API w celu uruchamiania skryptów oraz SNMP do komunikacji z zewnętrznymi narzędziami monitorującymi.	
23.	Serwisowalność	Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych. Macierz musi umożliwiać zdalne zarządzanie oraz automatyczne informowanie centrum serwisowego o awarii. Zgłoszenia usterek muszą być akceptowane zarówno drogą email jak również drogą telefoniczną.	
24.	Gwarancja, wsparcie serwisowe	1) Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta na terenie RP. 2) Macierz dyskowa musi zostać objęta **minimum 60 miesięcznym okresem gwarancji** (parametr oceniany) w trybie **on-site** z gwarantowanym czasem reakcji w ciągu 60 min od momentu zgłoszenia usterki. 3) Uszkodzone dyski po awarii pozostają u Zamawiającego bez konieczności zwrotu do serwisu/producenta. 4) Zgłoszenia usterek muszą być akceptowane zarówno drogą email (w ofercie należy podać dedykowany adres email do zgłoszeń serwisowych) jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.). 5) Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta. 6) Usługi gwarancyjne muszą być świadczone przez organizację serwisową producenta sprzętu posiadającą certyfikat ISO co najmniej 9001:2015. 7) Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków: - możliwość pobierania najnowszego firmware; - dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń; - dostęp do centrum pomocy technicznej producenta; - otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware; - otrzymywanie poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy	

5. Dostawa i wdrożenie oprogramowania do wykonywania kopii zapasowych wraz z usługą chmurową

Minimalne parametry techniczne:

Lp.	Opis przedmiotu zamówienia/ parametry wymagane	Parametr oferowany
1.	Wymagania minimalne:	
2.	Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji	
3.	Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012	
4.	Vmware vSphere min. w wersjach v5.5-7.0.3	
5.	Nutanix AHV 5.15, 5.20 (LTS)	
6.	Maszyny fizyczne: Windows Server 2022, 2019, 2016, 2012R2, 2012	

7.	Microsoft 365 (Exchange online, One Drive for Business, Sharepoint, Teams)	
8.	Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V	
9.	Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:	
10.	na serwerze Windows lub Linux	
11.	jako maszyna wirtualna Vmware	
12.	jako maszyna wirtualna Amazon	
13.	na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital	
14.	Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS	
15.	Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania	
16.	Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).	
17.	Licencjonowanie – wymaga się dostarczenia min. 6 licencji	
18.	Wszystkie funkcje i komponenty oprogramowania dla środowisk Vmware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariancie wieczystym, w którym licencja nie ma terminu ważności	
19.	Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 6 gniazd procesorów w obrębie środowiska	
20.	W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 1 roku wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania	
21.	W ramach dostawy wymagane jest dostarczenie licencji na ochronę X gniazd procesorów w hostach Vmware lub Hyper-V	
22.	W ramach dostawy wymagane jest dostarczenie licencji na ochronę X maszyn fizycznych z systemem operacyjnym Windows Server lub Linux (w wersji serwerowej)	
23.	W ramach dostawy wymagane jest dostarczenie licencji na ochronę X maszyn fizycznych z systemem operacyjnym Windows 10 Pro lub Ubuntu Desktop	
24.	Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska	
25.	Ochrona danych	
26.	Oprogramowanie musi posiadać funkcje backupu i replikacji:	
27.	Backup maszyn wirtualnych Vmware	
28.	Replikacja maszyn wirtualnych Vmware (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu	
29.	Backup maszyn wirtualnych Hyper-V	
30.	Replikacja maszyn wirtualnych Hyper-V (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu	
31.	Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych	
32.	Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie	

33.	Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu	
34.	Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym	
35.	"Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych	
36.	Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania	
37.	Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji	
38.	Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach	
39.	Optymalizacja wykorzystania miejsca na dane	
40.	Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:	
41.	Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane	
42.	Kompresja backupu, w tym konfigurowalny stopień kompresji	
43.	Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne	
44.	Spójność danych	
45.	Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:	
46.	Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux	
47.	Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu	
48.	Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji:	
49.	Microsoft Exchange 2013, 2016, 2019	
50.	Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022	
51.	Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki	
52.	Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V	
53.	Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania	
54.	Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji	
55.	Przywracanie danych	
56.	Oprogramowanie musi posiadać poniższe funkcje:	
57.	Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji	
58.	Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)	
59.	Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)	
60.	Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):	
61.	Microsoft Exchange	
62.	MS Active Directory	

63.	MS SQL	
64.	Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.	
65.	Wydajność	
66.	Oprogramowanie do backupu musi pozwalać na:	
67.	Tworzenie backupu I replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT	
68.	Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych	
69.	Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN	
70.	Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci	
71.	Wsparcie dla urządzeń oferujących dodatkową deduplikację danych	
72.	Zarządzanie	
73.	Oprogramowanie musi pozwalać na następujące formy zarządzania:	
74.	Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych	
75.	Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej	
76.	Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania	
77.	Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.	
78.	Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji	

usługa odmiejscowionej kopii zapasowej danych w chmurze min. 2TB, która zapewni regularne tworzenie, przechowywanie oraz odtwarzanie kopii zapasowych danych Zamawiającego. Usługa ta ma na celu zabezpieczenie danych przed utratą, zapewniając dostępność, integralność oraz bezpieczeństwo informacji zgodnie z obowiązującymi normami i przepisami prawnymi.

Kopia w chmurze będzie służyła do przechowywania strategicznych dokumentów i baz danych Zamawiającego.

Minimalne parametry techniczne:

Lp.	**Przedmiot zamówienia**	**Minimalne parametry wymagane**	**Parametr oferowany**
1.	Rodzaj chmury	Usługa musi być realizowana w chmurze prywatnej, z możliwością skalowania przestrzeni dyskowej zgodnie z potrzebami Zamawiającego.	
2.	Częstotliwość wykonywania kopii zapasowych:	Kopie zapasowe muszą być wykonywane regularnie, z częstotliwością co najmniej raz dziennie. Możliwość ustawienia harmonogramu tworzenia kopii zapasowych (np. codziennie, co godzinę, co tydzień, w zależności od krytyczności danych).	

3.	Szyfrowanie:	Dane muszą być szyfrowane w trakcie transferu (end-to-end encryption) oraz w spoczynku (encryption at rest) z użyciem algorytmu szyfrowania co najmniej AES-256.	
4.	Przestrzeń dyskowa:	Usługa musi umożliwiać elastyczne zarządzanie przestrzenią dyskową, z możliwością zwiększenia pojemności bez przerw w działaniu usługi.	
5.	Czas przechowywania kopii:	Przechowywanie kopii zapasowych przez minimum 30 dni z możliwością rozszerzenia tego okresu na żądanie Zamawiającego. Możliwość ustawienia polityk retencji (usuwania starszych kopii zapasowych po określonym czasie).	
6.	Funkcjonalności usługi	Usługa musi zapewniać automatyczne tworzenie kopii zapasowych zgodnie z ustalonym harmonogramem, bez konieczności ręcznego zarządzania procesem przez użytkownika. Zamawiający musi mieć zapewniony bezpieczny i szybki dostęp do kopii zapasowych w celu ich odtworzenia w razie awarii, a także możliwość przeglądania i zarządzania kopii zapasowych przez panel zarządzania. System musi generować raporty oraz powiadomienia dotyczące statusu kopii zapasowych, w tym powiadomienia o błędach, sukcesach oraz stanie przestrzeni dyskowej.	
7.	Wymagania dotyczące bezpieczeństwa	-Wymaga się, aby usługodawca spełniał najwyższe standardy bezpieczeństwa w zakresie ochrony danych, zgodnie z normami ISO/IEC 27001 lub równoważnymi. -Usługa musi spełniać wymogi przepisów prawa o ochronie danych osobowych, w tym RODO. -Możliwość przeprowadzania regularnych audytów bezpieczeństwa oraz dostępu do logów z działań związanych z tworzeniem i odtwarzaniem kopii zapasowych.	
8.	Gwarancja jakości	Usługa musi być świadczona zgodnie z uzgodnionymi parametrami SLA, zapewniającymi m.in. określony czas reakcji na awarie, czas odtworzenia danych oraz dostępność usługi.	
9.	Okres realizacji zamówienia	Okres świadczenia usługi wynosi 18 miesięcy.	

6. Dostawa oprogramowania wraz z instalacją i wdrożeniem oprogramowania do zarządzania infrastrukturą IT dla 80 licencji wieczystych:

Minimalne parametry techniczne:

Lp.	Przedmiot zamówienia	Minimalne parametry wymagane	Parametr oferowany
1.	Oprogramowanie:	1. Budowa modułowa,	

		2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. 3. Program umożliwia zmianę portu komunikacyjnego wykorzystywanego przez konsolę zarządzającą. 4. Silnik bazy danych musi być dostępny na licencji open source bez limitu ilości danych 5. Baza danych musi być darmowa i nie wymagać dodatkowego licencjonowania	
2.	Monitorowanie danych użytkownika:	1. historia aktywności 2. polityka korzystania z Internetu i aplikacji 3. dostęp do zewnętrznych nośników danych, 4. grupowanie informacji w oddzielnym oknie, co umożliwia usuwanie danych użytkownika zgodne z RODO bez konieczności usunięcia informacji o stacji roboczej, 5. dostęp do danych osobowych oraz danych z monitoringu zgodnie z RODO, 6. możliwość nadawania kontom różnych poziomów dostępu oraz uprawnień do funkcji Programu, grup urządzeń i użytkowników, 7. lista kont użytkowników i administratorów, może być synchronizowana z usługą typu Active Directory, przez szyfrowane połączenia, 8. konfiguracja haseł użytkownika 9. uwierzytelnianie logowań do konsoli z wykorzystaniem weryfikacji dwuskładnikowej	
3.	Funkcjonalności:	Oprogramowanie obsługuje m.in. 6 funkcjonalności: 1) Monitorowanie infrastruktury, 2) Inwentaryzacja sprzętu i oprogramowania, 3) Monitorowanie aktywności użytkowników, 4) Realizacja zdalnej pomocy użytkownikom, 5) Ochrona danych przed wyciekiem, 6) Wsparcie zarządzania czasem i analizowanie aktywności użytkowników	
4.	Monitorowanie infrastruktury:	1. Wykrywanie urządzeń w sieci poprzez skanowanie ping oraz arp-ping, 2. Wizualizacja urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki, tworzenie spersonalizowanych map z możliwością zablokowania mapy urządzeń przed przypadkową edycją, 3. Serwisy TCP/IP, HTTP, POP3, SMTP, FTP i inne wraz z możliwością definiowania własnych serwisów. Monitorowanie czasu ich odpowiedzi i procent utraconych pakietów, 4. Serwery pocztowe: - program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty, - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie, - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa 5. Monitorowanie serwerów WWW i adresów URL 6. Cykliczne monitorowanie czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS	

		7. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail 8. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID 9. Obsługa komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych 10. Monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych - ruchu sieciowego - podłączonych stacji roboczych – graficzna prezentacja panelu switcha - ruchu generowanego przez podłączone do portów stacje robocze 11. Monitor serwisów alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie, zatrzymanie lub zrestartowanie, 12. Wyświetlanie statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu 13. Monitorowanie stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano 14. Zarządzanie stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny 15. Wydajność systemów m.in. obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy, 16. Nakładanie na urządzenia liczników wydajności WMI oraz SNMP z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi, wyłączenie/restart komputera. 17. Administrator samodzielnie może konfigurować zdarzenia, lub wybrać zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. 18. Alarmy muszą pozwalać na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. 19. Oprogramowanie musi umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0	
5.	Inwentaryzacja sprzętu i oprogramowania,	1. Automatyczne gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych, min. modelu, procesora, pamięci, płyty głównej, napędów, 2. Umożliwienie odczytów parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe. 3. Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 4. Informacja o zainstalowanych aplikacjach oraz aktualizacjach systemu	

		5. Zbieranie informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. 6. Możliwość wysyłania powiadomienia np. e-mailem w przypadku jakiejkolwiek zmiany na urządzeniu 7. Możliwość odczytania numeru seryjnego (klucze licencyjne). 8. Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. 9. Możliwość przeglądania informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. 10. Możliwość utworzenia listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu). 11. Możliwość wymiany plików do i ze stacją roboczą poprzez funkcję Menedżera plików. *Moduł inwentaryzacji zasobów musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:* 12. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, 13. przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów, 14. tworzenia powiązań między zasobami a urządzeniami, 15. tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z funkcjonującą w Urzędzie Active Directory), wskazywanie osób odpowiedzialnych, 16. wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy, 17. definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości, 18. określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, 19. określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, 20. masową edycję atrybutów zasobów, 21. definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, 22. importu danych z zewnętrznego źródła (.CSV), 23. przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., 24. tworzenia powiązań między zasobami a dokumentami w relacji 1:N, 25. oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,	

		26. ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, 27. generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, 28. przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, 29. konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, 30. konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, 31. archiwizacji i porównywania audytów zasobów, 32. tworzenia kodów kreskowych dla zasobów, 33. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, 34. inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet, 35. możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android, 36. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), 37. definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data" z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja"). *Inwentaryzacja oprogramowania musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:* 3. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. 4. Informacje o aplikacjach używanych w organizacji. 11. Tworzenie własnych wzorców aplikacji. 12. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. 13. Informacje o komputerach, na których aplikacja została wykryta. 14. Zarządzanie posiadanymi licencjami. 15. Wskazywanie osób odpowiedzialnych za licencję. 16. Wskazanie użytkowników licencji, 17. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. 18. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.	

6.	Monitorowanie aktywności użytkowników:	1. Faktyczny czas aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy), 2. Otwarte procesy wraz z informacją o uruchomieniu na podwyższonych uprawnieniach, 3. Rzeczywiste użytkowanie programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność, 4. Informacja o edytowanych przez użytkownika dokumentach, 5. Historia pracy (cykliczne zrzuty ekranowe), 6. Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt), 7. Transfer sieciowy użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), 8. Wydruki m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program powinien mieć możliwość monitorowania kosztów wydruków, 9. Nagłówki przesyłanej w aplikacjach klienckich poczty e-mail. 10. Wykrywanie podejrzanej aktywności przez popularne „jigglery”, mającej na celu symulowanie faktycznej pracy. 11. Zdefiniowanie czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury. 12. Wyszczególnienie podejrzanej aktywności w raportach. 13. Wygenerowanie alarmu i wykonanie akcji po wykryciu podejrzanej aktywności. 14. Automatyczne włączenie zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności. 15. Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). 16. Blokowania ruchu na wskazanych portach TCP/IP, 17. Blokowanie pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem, 18. Prowadzenie rejestru naruszeń blokad, 19. Wysyłanie powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,	

		20. Przygotowanie zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika), 21. Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.	
7.	Realizacja zdalnej pomocy użytkownikom	1. Dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika, 2. Możliwość równoczesnego podłączenia do tego samego komputera kilku administratorów. 3. Oprogramowanie powinno zawierać komunikator (czat), który umożliwi prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów. Czat powinien pozwalać na: 4. zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej 5. rozmowy między „zwykłymi" użytkownikami 6. przesyłanie plików między rozmówcami w trybie online 7. tworzenie pokojów tematycznych, rozmów grupowych 8. oznaczanie kontaktów jako „ulubionych" na liście kontaktów 9. uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku, 10. Administrator powinien mieć możliwość tworzenia szkiców i archiwizowania komunikatów. Moduł pomocy zdalnej powinien umożliwiać: 11. pobieranie listy użytkowników z Active Directory, 12. wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym, 13. zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont, 14. zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez system zarządzania regułami widoczności zgłoszeń, 15. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń, 16. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy, 17. tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO, 18. automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,	

		19. definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji, 20. przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii, 21. procesowanie zgłoszeń użytkowników z wiadomości e-mail, 22. eksportowania listy zgłoszeń do plików CSV i XLSX, 23. integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0, 24. tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń, 25. wykonywanie operacji na wielu zgłoszeniach równocześnie, 26. dołączanie załączników do zgłoszeń, 27. rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, 28. szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, 29. wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia, 30. zrzuty ekranowe (podgląd pulpitu), 31. zdalną modyfikację rejestrów, 32. dystrybucję oprogramowania przez Agenty, 33. dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), 34. możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu, 35. możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy, 36. planowanie nieobecności pracowników helpdesk, 37. obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem, 38. generowanie raportów obsługi helpdesk, 39. zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu), 40. zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), 41. wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.	
8.	Ochrona danych przed wyciekiem	Blokowanie urządzeń i nośników danych: 1. możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. 2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.	

		3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. 4. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. 5. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender. 6. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker. 7. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker. 8. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu. 9. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu. 10. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender 11. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM. Zarządzanie prawami dostępu do urządzeń: 1) Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. 2) Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. 3) Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników. 4) Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. 5) Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane. Audyt operacji na plikach na urządzeniach przenośnych: 1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. 2. Podłączenie/odłączenie urządzenia przenośnego. 3. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. 4. Definiowanie reguł monitorowanych folderów w postaci list. Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.) Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.	
9.	Zarządzanie czasem i analizowanie aktywności użytkowników	1. Możliwość oznaczenia sesji aktywności jako czas prywatny gdy pracownik wykonuje czynności prywatne na sprzęcie firmowym. 2. Użytkownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje.	

		3. Zastosowane reguły powinny pozwalać zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. Dostęp powinien być realizowany przez przeglądarkę internetową, a strona powinna być wyświetlana w trybie jasnym lub ciemnym. 4. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. 5. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem. 6. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu. 7. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników. 8. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych. 9. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne. 10. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy. 11. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie). 12. Wskaźnik czasu poświęconego na aktywność produktywną. 13. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail. 14. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Rozrywka - predefiniowana lista kategorii z możliwością edycji. 15. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.	
10.	Gwarancja, wsparcie serwisowe	1. Wsparcie techniczne przez min. rok od dnia podpisania protokołu odbioru 2. W ramach wsparcia technicznego możliwość instalowania wszelkich aktualizacji oprogramowania, które zostaną wydane w czasie obowiązywania wsparcia, w tym aktualizacji obejmujących przejście na wyższą wersję oprogramowania. 3. Telefoniczne i mailowe wsparcie techniczne dla oprogramowania 4. Dokonywanie przez Producenta szczegółowej analizy zgłoszonych przypadków (logów). 5. Świadczenie przez Producenta pomocy w formie sesji zdalnych. 6. Czas reakcji na zgłoszenie nie dłuższy niż następny dzień roboczy. 7. Możliwość przedłużenia wsparcia o kolejny rok 8. Możliwość rozszerzenia oprogramowania o dodatkowe licencje i moduły	

7. Dostawa i instalacja i konfiguracja przełącznika dystrybucyjnego (zwany powyżej L3) – 1 szt.
Minimalne parametry techniczne:

Parametr	Charakterystyka (Wymagane minimalne)	Parametr oferowany
Przełącznik posiada:	1. min. 48 portów 1/10/25GE SFP28 bezpośrednio w obudowie przełącznika lub na karcie liniowej przełącznika modularnego 2. min. 6 portów definiowanych za pomocą wkładek QSFP, bezpośrednio w obudowie przełącznika lub na karcie liniowej, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps 3. Pamięć systemu min. 24 GB 4. Dysk SSD min. 64 GB	
Parametry wydajnościowe:	1. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3 2. Obsługiwana łączna przepływność (pasmo) min. 3,6 Tbps 3. Obsługiwana łączna przepustowość pakietowa przełącznika min. 1,6 bpps 4. opóźnienie przełączania pakietów nie większe niż 2 µs .	
Funkcjonalność warstwy L2:	1. Trunking IEEE 802.1Q VLAN; 2. Wsparcie dla min. 3967 sieci VLAN; 3. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN 4. Wsparcie sprzętowe dla minimum 256 tysięcy adresów MAC 5. IEEE 802.1s Multiple Spanning Tree (MST) 6. Statyczny i dynamiczny NAT 7. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree 8. Internet Group Management Protocol (IGMP)	
Funkcjonalność warstwy L3	1. Sprzętowe przełączanie pakietów w warstwie L3 2. Routing w oparciu o trasy statyczne 3. Routing w oparciu o OSPF, BGP 4. Wsparcie sprzętowe dla minimum 896 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP 5. Wsparcie dla IPv4 multicast w oparciu o protokół PIM-SM Sparse Mode I tryb SSM (Source Specific Multicast) 6. Wsparcie dla IGMPv3 oraz MSDP 7. Wsparcie sprzętowe dla minimum 32,000 tras multicastowych 8. Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking) 9. Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP) 10. Minimum 1000 wejściowych oraz min. 1000 wyjściowych wpisów dla ACL - access control list	
Wsparcie mechanizmów bezpieczeństwa w sieci:	1. Wsparcie ACL 2. Snooping 3. ARP Inspection	
Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:	1. Port zarządzający 100/1000 Mbps; 2. Port konsoli CLI; 3. Ping 4. Traceroute.	
Akcesoria:	1. 2 szt. wkładek QSFP-100G-LR4-S 2. 2 szt. patchcord LCLC-SM-50CM	

	3. 15 szt. składek SFP-10G-SR 4. 6 szt. wkładek SFP+ SFP-25G-SR.	
Zasilanie	1. 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej.	
Obudowa	1. maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19". W wypadku zastosowania przełącznika modularnego dopuszcza się większy rozmiar urządzenia (jednak nie większy niż 2U).	
Gwarancja:	1. min. 60 miesięcy 2. Gwarancja obejmuje wszystkie części składowe urządzenia.	
Serwis	1. Świadczony na miejscu u Zamawiającego 2. Opieka serwisowa 24 godziny na dobę 7 dni w tygodniu. 3. Czas reakcji na zgłoszenie awarii max. do 60 min. 4. Wymagany czas naprawy awarii 24 godziny od momentu zgłoszenia. W przypadku niemożliwego usunięcia awarii w przeciągu 24 godz. Wykonawca jest zobowiązany dostarczyć urządzenie zamienne, o parametrach nie gorszych, na czas usunięcia awarii. 5. Uszkodzone nośniki danych pozostają u Zamawiającego. 6. Kontakt z pracownikami serwisu będzie prowadzony w języku polskim.	

8. Dostawa i wdrożenie zarządzalnych przełączników sieciowych do utworzenia rdzenia sieci LAN – 6 szt.

Minimalne parametry techniczne:

LP.	Przedmiot zamówienia	Opis przedmiotu zamówienia/ parametry wymagane	Parametr oferowany
1.	Typ i liczba portów	48 portów 10/100/1000BaseT RJ-45 + uplink 4x10G SFP	
2.	Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:	- Gigabit Ethernet 1000Base-SX, - Gigabit Ethernet 1000Base-LX/LH, - 10Gigabit Ethernet 10GBase-SR, - 10Gigabit Ethernet 10GBase-LR, - • 10Gigabit Ethernet typu twinax (SFP+ - SFP+)	
3.	Urządzenie posiada funkcjonalność zarządzania przez 1 adres IP grupą (klastrem)	do 8 urządzeń pochodzących z tej samej rodziny przełączników połączonych portami uplinkowymi,	
4.	Zasilanie i chłodzenie	- Urządzenie wyposażone jest w wbudowany zasilacz AC230V	
Parametry wydajnościowe			
5.	Przepustowość przełącznika (switching bandwidth)	min. 176 Gb/s (full duplex),	
6.	Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3	min. 77.38 Mpps	
7.	Pamięć DRAM	Min. 512 MB	
8.	Pamięć flash	256 MB	
9.	Wielkość bufora pakietów	1.5 MB	
10.	Obsługa	- 256 aktywnych sieci VLAN - 15000 adresów MAC	

		- 16 statycznych tras IPv4 - 16 statycznych tras IPv6 - 64 interfejsów SVI L3 - Obsługa MTU-L3 9198B - Obsługa ramek Ethernet Jumbo 10240B - 1024 grupy IGMP - 6 połączeń zagregowanych typu „port channel” - 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP - Ilość wpisów w listach kontroli dostępu Security ACL – 600 - • ilość wpisów w listach kontroli dostępu QoS ACL – 600	
11.	Porty dostępowe przełącznika posiadają zgodność ze standardem	standard IEEE 802.3az EEE (Energy Efficient Ethernet)	
12.	Obsługa protokołu	NTP, LLDP i LLDP-MED	
13.	Obsługa	IGMPv1/2/3 i MLDv1/2 Snooping	
14.	Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC	Tak	
15.	Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad	Tak	
16.	Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego	Tak	
17.	Możliwość uruchomienia funkcji serwera DHCP	Tak	
18.	Mechanizmy związane z bezpieczeństwem sieci:	- Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level), - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL, - Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego	

		dostępu do sieci dla użytkowników bez suplikanta 802.1X, - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, - Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X, - Możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem (multidomain authentication), - Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, - Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www), - Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, - Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, - Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP), - Funkcja Private VLAN,	
19.	Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:	- sprawdzanie autentyczności oprogramowania przed uruchomieniem urządzenia, - bezpieczna sekwencja uruchamiania, - sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.	
20.	Mechanizmy związane z zapewnieniem jakości usług w sieci:	- Implementacja 4 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, - Implementacja algorytmu Shaped Round Robin dla obsługi kolejek, - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), - Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów:	

		źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, - Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z możliwością skonfigurowania minimum 64 różnych ograniczeń, - Kontrola sztormów dla ruchu broadcast/multicast/unicast, - Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;	
21.	Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6	Tak	
22.	Przełącznik umożliwia lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizm SPAN z możliwością obsługi do 4 sesji monitorujących,	Tak	
23.	Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.),	Tak	
24.	Obsługa protokołu sFlow dla wszystkich portów fizycznych uplinkowych i downlinkowych dla ruchu w kierunku wejściowym i wyjściowym z możliwością skonfigurowania 2 różnych kolektorów ruchu sFlow,	Tak	
Zarządzanie			

25.	Port konsoli,	Tak	
26.	Dostęp bezprzewodowy Bluetooth do interfejsu zarządzającego urządzenia (telnet, ssh) przez zastosowanie zewnętrznego urządzenia Bluetooth podłączonego do portu USB przełącznika,	Tak	
27.	Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,	Tak	
28.	Obsługa protokołów	SNMPv3, SSHv2, https, syslog,	
29.	Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia	Tak/podać	
30.	Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki;	Tak/podać	
31.	Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU	Tak/podać	
32.	Akcesoria	1. 5 szt. wkładek SFP-10G-SR 2. 5 szt. Patchord LCLC-MM-OM3-50CM	
Warunki Gwarancji i serwisu			
33.	Gwarancja dla wszystkich urządzeń należących do przedmiotu zamówienia min 12 m-ce liczone od dnia podpisania protokołu odbioru		
34.	Gwarancja obejmuje wszystkie części składowe urządzenia.		
35.	Gwarantowany czas naprawy awarii 24 godziny od momentu zgłoszenia. W przypadku niemożliwego usunięcia awarii w przeciągu 24 godz.		

	Wykonawca jest zobowiązany dostarczyć urządzenie zamienne, o parametrach nie gorszych, na czas usunięcia awarii.	
36.	Świadczony na miejscu u Zamawiającego	
37.	Opieka serwisowa 24 godziny na dobę 7 dni w tygodniu.	
38.	Czas reakcji na zgłoszenie max. 60 min, rozpoczęcie naprawy w ciągu 24 godz. od zgłoszenia.	
39.	Kontakt z pracownikami serwisu będzie prowadzony w języku polskim.	

9. Dostawa, instalacja oraz podłączenie zasilacza awaryjnego UPS z kartą SNMP

Minimalne parametry techniczne:

LP.	Przedmiot zamówienia	Opis przedmiotu zamówienia/ parametry wymagane	Parametry oferowane (podać)
1.	Moc	min. 3000VA/2700W	
2.	Obudowa	Możliwość montażu na stojąco jak i w szafie rack 19"	
3.	Faza	1 faza z uziemieniem	
4.	Typ baterii	12V/9AH	
5.	Ilość baterii	min. 4	
6.	Czas ładowania	max. 4 godzin regeneracji do 90% pojemności	
	Wejście		
7.	Napięcie Zakres napięcia Zakres częstotliwości	208/220/230/240 VAC 110-300 VAC ± 5% przy 50% obciążenia 160-300 VAC ± 5% przy 100% obciążenia 40/70 Hz (automatyczne wykrywanie)	
	Wyjście		
8.	Napięcie wyjściowe Regulacja napięcia AC (tryb baterii) Zakres częstotliwości (tryb baterii) Max czas przełączenia UPS w tryb zasilania akumulatorowego Kształt fali (tryb baterii)	208/220/230/240 VAC ±1% 57~63 Hz lub 50 Hz ± 0.1 Hz max. 4 ms Czysta fala sinusoidalna	
9.	Możliwość wymiany baterii podczas pracy	Tak	
10.	Zabezpieczenie przed przeciążeniem, rozładowaniem i przeładowaniem	Tak	
	Wskaźniki		
11.	Wyświetlacz LCD	Poziom obciążenia, poziom naładowania akumulatora, tryb AC, tryb akumulatora, tryb obejścia i wskaźnik usterki	
	Alarm:		
12.	Tryb baterii	Dźwięk co 4 s	
13.	Niski poziom naładowania baterii	Dźwięk co 1 s	
14.	Przeciążenie	Dźwięk dwa razy na sekundę	
15.	Usterka	Ciągły sygnał dźwiękowy	
	Środowisko		

16.	Działanie w warunkach wilgotności	20-90% wilgotności względnej przy 0-40°C (bez kondensacji)	
17.	Poziom hałasu	Mniej niż 50 dBA w odległości 1 metra	
18.	Czas podtrzymania w zależności od obciążenia	min. 11,5 min przy 50% obciążeniu bez dodatkowych akumulatorów	
19.	Wbudowany stabilizator AVR	Tak	
20.	Automatyczny restart podczas przywracania napięcia AC	Tak	
21.	Funkcja zimnego startu	Tak	
22.	Ładowanie w trybie wyłączenia	Tak	
23.	Wbudowany port komunikacyjny	USB, RJ, SNMP	
24.	Karta SNMP	Tak	
25.	Złącze wejście AC Złącze wyjścia AC	min. 1x IEC 320 x14 min. 1x IEC 320 C19 min. 6x IEC 320 C13	
	Zarządzanie		
26.	Interfejs RS 232/USB	Wsparcie Windows 2000/2003/XP/Vista/2008, Windows 7,8,10 Linux i MAC	
	Warunki Gwarancji i serwisu		
27.	Gwarancja dla wszystkich urządzeń należących do przedmiotu zamówienia 24 m-ce liczone od dnia podpisania protokołu odbioru	Tak/podać	
28.	Gwarancja obejmuje wszystkie części składowe urządzenia.	Tak/podać	
29.	Gwarantowany czas naprawy awarii 24 godziny od momentu zgłoszenia. W przypadku niemożliwego usunięcia awarii w przeciągu 24 godz. Wykonawca jest zobowiązany dostarczyć urządzenie zamienne, o parametrach nie gorszych, na czas usunięcia awarii.	Tak/podać	
30.	Świadczony na miejscu u Zamawiającego	Tak/podać	
31.	Opieka serwisowa 24 godziny na dobę 7 dni w tygodniu.	Tak/podać	
32.	Czas reakcji na zgłoszenie max. 60 min, rozpoczęcie naprawy w ciągu 24 godz. od zgłoszenia.	Tak/podać	
33.	Kontakt z pracownikami serwisu będzie prowadzony w języku polskim.	Tak/podać	

10. Dostawa wraz z montażem i uruchomieniem dysków 12TB przeznaczonych do wykonywania kopii zapasowych – 5 szt.

Minimalne parametry techniczne:

LP.	Przedmiot zamówienia	Minimalne parametry wymagane	Parametr oferowany
1	Pojemność	12 TB	
2	Interfejs	SATA III (6 Gb/s)	
3	Rozmiar	3,5"	
4	Prędkość obrotowa	7200 RPM	
5	Pamięć cache	256 MB	

6	Kompatybilność	Kompatybilność z systemami NAS, RAID, systemami przechowywania danych o wysokiej wydajności	
7	Gwarancja	36 miesięcy gwarancji	

……

(podpis wykonawcy lub osób uprawnionych do występowania w jego imieniu)

Załącznik 2 b

Wykaz oferowanego oprogramowania wraz z szczegółowym opisem technicznym

Cz. II - dostawa oprogramowania do monitorowania infrastrukturą sieci informatycznej i urządzeń dla jednostki podległej oraz dostawa usług chmurowych w ramach zabezpieczenia poczty i stron internetowych Gminy.

UWAGA!

Zamawiający wymaga dołączenia wykazu oferowanego sprzętu do formularza ofertowego. W pozycji parametry oferowane należy umieścić opis techniczny umożliwiający Zamawiającemu jednoznaczne określenie szczególnych cech produktu oraz wymagane prawem certyfikaty, deklaracje zgodności CE, instrukcje obsługi sprzętu, dokumenty gwarancyjne, celem sprawdzenia zgodności oferowanego produktu.

W przypadku nie dołączenia wymienionego powyżej wykazu do formularza oferty oferta podlega odrzuceniu jako niezgodna z zapisami swz.

1. **Oprogramowanie do zarządzania infrastrukturą IT na 31 licencji**
   Zamawiający wymaga dostarczenia oprogramowania wraz z licencjami spełniającego poniższe graniczne minimalne parametry techniczne.

Lp.	Przedmiot zamówienia	Minimalne parametry wymagane	Parametr oferowany
1.	Oprogramowanie:	1. Budowa modułowa, 2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. 3. Program umożliwia zmianę portu komunikacyjnego wykorzystywanego przez konsolę zarządzającą. 4. Silnik bazy danych musi być dostępny na licencji open source bez limitu ilości danych 5. Baza danych musi być darmowa i nie wymagać dodatkowego licencjonowania	
2.	Monitorowanie danych użytkownika:	1. historia aktywności 2. polityka korzystania z Internetu i aplikacji 3. dostęp do zewnętrznych nośników danych, 4. grupowanie informacji w oddzielnym oknie, co umożliwia usuwanie danych użytkownika zgodne z RODO bez konieczności usunięcia informacji o stacji roboczej, 5. dostęp do danych osobowych oraz danych z monitoringu zgodnie z RODO, 6. możliwość nadawania kontom różnych poziomów dostępu oraz uprawnień do funkcji Programu, grup urządzeń i użytkowników, 7. lista kont użytkowników i administratorów, może być synchronizowana z usługą typu Active Directory, przez szyfrowane połączenia, 8. konfiguracja haseł użytkownika 9. uwierzytelnianie logowań do konsoli z wykorzystaniem weryfikacji dwuskładnikowej	
3.	Funkcjonalności:	Oprogramowanie obsługuje min. 6 funkcjonalności: 1. Monitorowanie infrastruktury, 2. Inwentaryzacja sprzętu i oprogramowania, 3. Monitorowanie aktywności użytkowników, 4. Realizacja zdalnej pomocy użytkownikom, 5. Ochrona danych przed wyciekiem, 6. Wsparcie zarządzania czasem i analizowanie aktywności użytkowników	

4.	Monitorowanie infrastruktury:	1. Wykrywanie urządzeń w sieci poprzez skanowanie ping oraz arp-ping, 2. Wizualizacja urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki, tworzenie spersonalizowanych map z możliwością zablokowania mapy urządzeń przed przypadkową edycją, 3. Serwisy TCP/IP, HTTP, POP3, SMTP, FTP i inne wraz z możliwością definiowania własnych serwisów. Monitorowanie czasu ich odpowiedzi i procent utraconych pakietów, 4. Serwery pocztowe: - program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty, - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie, - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa 5. Monitorowanie serwerów WWW i adresów URL 6. Cykliczne monitorowanie czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS 7. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail 8. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID 9. Obsługa komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych 10. Monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych - ruchu sieciowego - podłączonych stacji roboczych – graficzna prezentacja panelu switcha - ruchu generowanego przez podłączone do portów stacje robocze 11. Monitor serwisów alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie, zatrzymanie lub zrestartowanie, 12. Wyświetlanie statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu 13. Monitorowanie stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano 14. Zarządzanie stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny 15. Wydajność systemów m.in. obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy, 16. Nakładanie na urządzenia liczników wydajności WMI oraz SNMP z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki	

		SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi, wyłączenie/restart komputera. 17. Administrator samodzielnie może konfigurować zdarzenia, lub wybrać zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. 18. Alarmy muszą pozwalać na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. 19. Oprogramowanie musi umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0	
5.	Inwentaryzacja sprzętu i oprogramowania,	1. Automatyczne gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych, min. modelu, procesora, pamięci, płyty głównej, napędów, 2. Umożliwienie odczytów parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe. 3. Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 4. Informacja o zainstalowanych aplikacjach oraz aktualizacjach systemu 5. Zbieranie informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. 6. Możliwość wysyłania powiadomienia np. e-mailem w przypadku jakiejkolwiek zmiany na urządzeniu 7. Możliwość odczytania numeru seryjnego (klucze licencyjne). 8. Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. 9. Możliwość przeglądania informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. 10. Możliwość utworzenia listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu). 11. Możliwość wymiany plików do i ze stacją roboczą poprzez funkcję Menedżera plików. *Moduł inwentaryzacji zasobów musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:* 12. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, 13. przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów, 14. tworzenia powiązań między zasobami a urządzeniami, 15. tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i	

		zsynchronizowanymi z funkcjonującą w Urzędzie Active Directory), wskazywanie osób odpowiedzialnych, 16. wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy, 17. definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości, 18. określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, 19. określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, 20. masową edycję atrybutów zasobów, 21. definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, 22. importu danych z zewnętrznego źródła (.CSV), 23. przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., 24. tworzenia powiązań między zasobami a dokumentami w relacji 1:N, 25. oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., 26. ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, 27. generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, 28. przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, 29. konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, 30. konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, 31. archiwizacji i porównywania audytów zasobów, 32. tworzenia kodów kreskowych dla zasobów, 33. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, 34. inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet, 35. możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android, 36. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), 37. definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).	

		Inwentaryzacja oprogramowania musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez: 1) Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. 2) Informacje o aplikacjach używanych w organizacji. 3) Tworzenie własnych wzorców aplikacji. 4) Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. 5) Informacje o komputerach, na których aplikacja została wykryta. 6) Zarządzanie posiadanymi licencjami. 7) Wskazywanie osób odpowiedzialnych za licencję. 8) Wskazanie użytkowników licencji, 9) Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. 10) Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.	
6.	Monitorowanie aktywności użytkowników:	1. Faktyczny czas aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy), 2. Otwarte procesy wraz z informacją o uruchomieniu na podwyższonych uprawnieniach, 3. Rzeczywiste użytkowanie programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność, 4. Informacja o edytowanych przez użytkownika dokumentach, 5. Historia pracy (cykliczne zrzuty ekranowe), 6. Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt), 7. Transfer sieciowy użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), 8. Wydruki m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program powinien mieć możliwość monitorowania kosztów wydruków, 9. Nagłówki przesyłanej w aplikacjach klienckich poczty e-mail. 10. Wykrywanie podejrzanej aktywności przez popularne „jigglery", mającej na celu symulowanie faktycznej pracy. 11. Zdefiniowanie czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury. 12. Wyszczególnienie podejrzanej aktywności w raportach.	

		13. Wygenerowanie alarmu i wykonanie akcji po wykryciu podejrzanej aktywności. 14. Automatyczne włączenie zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności. 15. Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). 16. Blokowania ruchu na wskazanych portach TCP/IP, 17. Blokowanie pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem, 18. Prowadzenie rejestru naruszeń blokad, 19. Wysyłanie powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady, 20. Przygotowanie zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika), 21. Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.	
7.	Realizacja zdalnej pomocy użytkownikom	1. Dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika, 2. Możliwość równoczesnego podłączenia do tego samego komputera kilku administratorów. 3. Oprogramowanie powinno zawierać komunikator (czat), który umożliwi prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów. Czat powinien pozwalać na: 1) zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej 2) rozmowy między „zwykłymi" użytkownikami 3) przesyłanie plików między rozmówcami w trybie online 4) tworzenie pokojów tematycznych, rozmów grupowych 5) oznaczanie kontaktów jako „ulubionych" na liście kontaktów 6) uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku, 7) Administrator powinien mieć możliwość tworzenia szkiców i archiwizowania komunikatów. Moduł pomocy zdalnej powinien umożliwiać: 1) pobieranie listy użytkowników z Active Directory, 2) wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym, 3) zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,	

		4) zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez system zarządzania regułami widoczności zgłoszeń, 5) zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń, 6) zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy, 7) tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO, 8) automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników, 9) definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji, 10) przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii, 11) procesowanie zgłoszeń użytkowników z wiadomości e-mail, 12) eksportowania listy zgłoszeń do plików CSV i XLSX, 13) integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0, 14) tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń, 15) wykonywanie operacji na wielu zgłoszeniach równocześnie, 16) dołączanie załączników do zgłoszeń, 17) rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, 18) szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, 19) wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia, 20) zrzuty ekranowe (podgląd pulpitu), 21) zdalną modyfikację rejestrów, 22) dystrybucję oprogramowania przez Agenty, 23) dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), 24) możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu, 25) możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy, 26) planowanie nieobecności pracowników helpdesk, 27) obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem, 28) generowanie raportów obsługi helpdesk, 29) zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),	

		30) zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), 31) wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.	
8.	Ochrona danych przed wyciekiem	Blokowanie urządzeń i nośników danych: 1. możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. 2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. 3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. 4. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. 5. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender. 6. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker. 7. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker. 8. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu. 9. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu. 10. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender 11. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM. Zarządzanie prawami dostępu do urządzeń: 1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. 2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków itp. 3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników. 4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. 5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane. Audyt operacji na plikach na urządzeniach przenośnych: 5. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. 6. Podłączenie/odłączenie urządzenia przenośnego. 7. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. 8. Definiowanie reguł monitorowanych folderów w postaci list. Monitorowanie operacji na plikach na	

		udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.) Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.	
9.	Zarządzanie czasem i analizowanie aktywności użytkowników	1. Możliwość oznaczenia sesji aktywności jako czas prywatny gdy pracownik wykonuje czynności prywatne na sprzęcie firmowym. 2. Użytkownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. 3. Zastosowane reguły powinny pozwalać zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. 4. Dostęp powinien być realizowany przez przeglądarkę internetową, a strona powinna być wyświetlana w trybie jasnym lub ciemnym. 5. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. 6. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem. 7. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu. 8. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników. 9. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych. 10. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne. 11. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy. 12. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie). 13. Wskaźnik czasu poświęconego na aktywność produktywną. 14. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail. 15. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Rozrywka - predefiniowana lista kategorii z możliwością edycji. 16. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.	
10.	Gwarancja, wsparcie serwisowe	1. Wsparcie techniczne przez min. rok od dnia podpisania protokołu odbioru 2. W ramach wsparcia technicznego możliwość instalowania wszelkich aktualizacji oprogramowania, które zostaną wydane w czasie obowiązywania wsparcia, w tym aktualizacji obejmujących przejście na wyższą wersję oprogramowania. 3. Telefoniczne i mailowe wsparcie techniczne dla oprogramowania	

		4. Dokonywanie przez Producenta szczegółowej analizy zgłoszonych przypadków (logów). 5. Świadczenie przez Producenta pomocy w formie sesji zdalnych. 6. Czas reakcji na zgłoszenie nie dłuższy niż następny dzień roboczy. 7. Możliwość przedłużenia wsparcia o kolejny rok 8. Możliwość rozszerzenia oprogramowania o dodatkowe licencje i moduły	

2. **Usługa zabezpieczenia poczty na 24 miesiące**
   1. Zamawiający w ramach przedmiotu zamówienia wymaga dostarczenia usługi zabezpieczenia poczty spełniającej poniższe minimalne parametry techniczne:

Lp.	Minimalne parametry wymagane		Parametr oferowany
1.	system ochrony poczty elektronicznej przed wiadomościami niepożądanymi typu spam, wirusy i oprogramowanie złośliwe, phishing, wyłudzenia, podszywanie, manipulacja tożsamością i inne zagrożenia bezpieczeństwa informatycznego.		
2.	System filtrujący, portal konfiguracji polityki bezpieczeństwa, system zarządzania i raportowania dostępne jako usługi chmurowe		
3.	ochrona przed wiadomościami niepożądanymi za pomocą filtracji poczty przychodzącej i ochronę reputacji własnego systemu pocztowego przez filtrację poczty wychodzącej.		
4.	Przekierowanie ruchu pocztowego do chmury obsługiwane na poziomie konfiguracji rekordów Mail Exchange (MX) w systemie DNS.		
5.	Chmurowy system ochrony powinien umożliwiać obsługę wielu domen pocztowych jednocześnie (nie mniej niż 15).		
6.	Chmurowy system ochrony powinien zapewniać ochronę przed wolumetrycznymi atakami Denial-of-Service		
Funkcjonalność filtracji poczty przychodzącej:			
7.	Filtracja wiadomości typu spam:	- wszystkie przychodzące wiadomości powinny być klasyfikowane pod kątem prawdopodobieństwa, że jest to wiadomość typu spam - klasyfikacja powinna być automatyczna i pracować bez ingerencji administratora lub konfiguracji - możliwość zaprogramowania poziomu tolerancji na spam: od całkowitej blokady do całkowitej akceptacji wszystkich wiadomości sklasyfikowanych jako spam - możliwość zaprogramowania typu reakcji na spam: co najmniej „blokada", „kwarantanna", „akceptacja",	
8.	Filtracja wiadomości ze względu na kategorię komunikacji:	- oprócz filtrowania wiadomości typu spam system powinien rozpoznawać inne, często niejednoznaczne kategorie komunikacji, co najmniej: komunikację służbową, komunikację handlową, komunikację marketingową, komunikację związaną z listami mailingowymi, komunikację związaną z mediami społecznościowymi, komunikację rozsyłaną masowo - dla każdej rozpoznanej kategorii powinna być możliwość zaprogramowania reakcji, co najmniej: „blokada", „kwarantanna", „akceptacja"	

9.	Filtracja wiadomości zawierających wirusy i oprogramowanie złośliwe, zagrożenia ATP i zagrożenia Zero-Day	- możliwość skanowania przez silnik antywirusowy - możliwość skanowania przez silnik sandboxingowy: wykrywanie zagrożeń zamaskowanych typu *Advanced Persistent Threats* (ATP) i zagrożeń typu *Zero-Day* - polityka skanowania ATP powinna umożliwiać konfigurację wyjątków opartych na adresach IP, na adresach nadawców i odbiorców poczty elektronicznej	
10.	Filtracja wiadomości phishingowych, wiadomości związanych z wyłudzeniami, ochrona przed złośliwymi adresami URL:	- możliwość filtrowania wiadomości pod kontem phishingu, inżynierii socjalnej, próbami wyłudzeń i kradzieży tożsamości - możliwość filtrowania i ochrony adresów URL zawartych w wiadomościach przed złośliwym wykorzystaniem i zmianą zawartości po dostarczeniu do odbiorcy (*link protection, typosquatting protection*	
11.	Filtracja wiadomości na podstawie informacji geograficznych (GeoIP) i językowych	- możliwość blokowania lub umieszczania w kwarantannie poczty przychodzącej z wybranego kraju (np. z Somalii) - możliwość blokowania lub umieszczania w kwarantannie poczty w określonym języku (np. chińskim)	
12.	Filtracja wiadomości na podstawie zawartości - możliwość blokowania lub umieszczania w kwarantannie	- wiadomości z załącznikami o określonej nazwie lub o okroślonym typie MIME - wiadomości z załącznikami zaszyfrowanymi, co najmniej: archiwa takie jak ZIP, pliki Microsoft Office, pliki PDF - wiadomości zawierających wskazane słowa kluczowe w nagłowkach, temacie, zawartości lub w załącznikach	
13.	Filtracja wiadomości przychodzących na podstawie polityk DNS, SPF, DKIM i DMARC	- możliwość weryfikacji domeny nadawcy: blokowanie nadawców z nieskonfigurowanym rekordem PTR - możliwość weryfikacji nadawcy za pomocą polityki *Sender Policy Framework (SPF)* - możliwość weryfikacji nadawcy za pomocą polityki *Domain Key Identified Email (DKIM)* - możliwość weryfikacji nadawcy za pomocą polityki *Domain Based Message Authentication (DMARC)*	
Funkcjonalność związana z kwarantanną i buforowaniem wiadomości:			
14.	Kwarantanna i buforowanie wiadomości	- możliwość pracy z kwarantanną indywidualną, skonfigurowaną i dostępną per użytkownik - możliwość pracy z kwarantanną globalną	

15.	Buforowanie i udostępnianie wiadomości w przypadku awarii docelowego serwera pocztowego:	- odbiór i buforowanie wiadomości przychodzących do czasu usunięcia awarii docelowego serwera pocztowego (co najmniej 96 godzin) - udostępnienie zbuforowanych wiadomości użytkownikom za pomocą interfejsu webowego, pozwalającego odczytywać i odpowiadać na wiadomości w czasie awarii - synchronizację wiadomości z serwerem docelowym po usunięciu awarii	
16.	Buforowanie wiadomości przychodzących	- system powinien umożliwiać administratorowi przeszukiwanie przychodzących transmisji, co najmniej z ostatnich 30 dni - system powinien umożliwiać zmianę decyzji blokującej wiadomość z ostatnich 30 dni i dostarczenie zablokowanej wiadomości do odbiorcy	
Funkcjonalność filtracji poczty wychodzącej:			
17.	skanowanie wiadomości wychodzących:	- wiadomości zawierające wirusy powinny być blokowane - wiadomości podejrzane o spam powinny być blokowane lub poddane kwarantanni	
18.	Filtracja wiadomości wychodzących z możliwością kwarantanny:	- filtracja nazw i typów MIME załączonych plików - filtracja zaszyfrowanych i chronionych hasłem plików archiwów, plików Microsoft Office, plików PDF - filtracja na podstawie słów kluczowych w nagłowkach, temacie, zawartości, załącznikach, adresie nadawcy lub adresie odbiorcy	
Monitorowanie i raportowanie:			
19.	Możliwość wyświetlania raportów i eksportu raportowanych danych do pliku, co najmniej	- analiza ruchu pocztowego przychodzącego i wychodzącego w zadanym czasie: liczba wiadomości przychodzących, zablokowanych, zablokowanych ze względu na spam, wirusy lub zagrożenia ATP - analiza użytkowników: odbiorcy i nadawcy spamu i wirusów analiza użytkowników: najczęściej blokowani odbiorcy i nadawcy	
Funkcjonalność związana z integracją z systemami zewnętrznymi			
20.	Możliwość integracji z zewnętrznym systemem monitorowania	- wsparcie dla protokołu SYSLOG z szyfrowaniem w standardzie TLS	
Warunki Gwarancji i serwisu			
21.	Wsparcie techniczne musi zapewniać dostęp do poprawek oprogramowania oraz wsparcia technicznego producenta z czasem reakcji nie dłuższym niż 2 godziny od momentu zgłoszenia problemu		
22.	Wymagana jest dostępność usługi w trybie 8x5 w godzinach od 8:00 do 15:00 (e-mail; telefon) 24x7 poprzez zgłoszenie Email.		

3. Usługa zabezpieczenia serwisu www na 24 miesiące:

Zamawiający w ramach przedmiotu zamówienia wymaga dostarczenia do Zamawiającego usługi zabezpieczenia serwisu stron internetowych na 24 miesiące spełniającego minimalne parametry techniczne opisane poniżej:

Lp.	Opis przedmiotu zamówienia/ Minimalne parametry wymagane	Parametr oferowany
1.	Dostęp do platformy umożliwiającej ochronę wybranych stron internetowych.	
2.	Dostarczona usługa w postaci subskrypcji ważnej 24 miesiące powinna: posiadać funkcje ochrony Web Application Firewall (WAF) i Captcha, - zapewniać zaawansowaną ochronę przed atakami DDoS, - umożliwiać dostęp do globalnej sieć dostarczania treści (CDN), - zapewniać szyfrowanie i optymalizację SSL, - obsługiwać IPv6, - automatycznie buforować treści statyczne, - zapewnić utrzymanie statycznych elementów serwisu online również w przypadku awarii serwera, - zapewnić zabezpieczenie przed kopiowaniem treści, w tym tekstu, obrazów i adresów e-mail przed mechanizmami automatycznie zbierającymi treści z Internetu, - uniemożliwiać dostępu do serwisu z indywidualnych adresów IP, zakresów adresów, lub z określonych krajów.	
3.	poprawa wydajności strony internetowej	
4.	działa jako autorytatywny serwer DNS, co odpowiada za kierowanie ruchu do strony internetowej.	
5.	możliwość samodzielnego zarządzania usługą poprzez panel administracyjny, możliwość skalowania i elastycznego dobierania funkcjonalności,	
6.	zapewnienie regionalnego (PL) podstawowego wsparcia technicznego w minimalnym przedziale od poniedziałku do piątku w godzinach min. 08:00 – 15:00.	

……

(podpis wykonawcy lub osób uprawnionych do występowania w jego imieniu)

Załącznik nr 3

Oświadczenie Wykonawcy

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

o niepodleganiu wykluczeniu

z uwzględnieniem przesłanek na podstawie art.7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego z postępowania o udzielenie zamówienia pn.: ***„Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko."***

Gmina Miastko
ul. Grunwaldzka 1
77-200 Miastko

Wykonawca:

.....

.....
(pełna nazwa)

reprezentowany przez

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

Adres/siedziba…..……

NIP……

REGON……
(w przypadku składania oferty przez podmioty występujące wspólnie podać nazwy (firmy) i dokładne adresy wszystkich członków konsorcjum)

Na potrzeby niniejszego postępowania, oświadczam, co następuje:

1. Oświadczenie dotyczące wykonawcy

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

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

(podpis wykonawcy lub osób uprawnionych do występowania w jego imieniu)

2) **Oświadczam**, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. 108 ust. 1 w związku z przesłankami określonymi w ust. 1 pkt……..przywołanego artykułu.

(wskazać pkt w art. 108 ust. 1 Pzp - przypisany do przesłanki lub przesłanek, które wystąpiły)

Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. Art. 110 ust. 2 Pzp podjąłem następujące środki naprawcze:

……

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

(podpis wykonawcy lub osób uprawnionych do występowania w jego imieniu)

2. Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

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

(podpis wykonawcy lub osób uprawnionych do występowania w jego imieniu)

(Podpisać właściwe oświadczenie wskazane w pkt 1 –3, pozostałe wykreślić)

3. Oświadczenie dotyczące podanych informacji

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

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

(podpis wykonawcy lub osób uprawnionych do występowania w jego imieniu)

Załącznik nr 4

Oświadczenie wykonawcy

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych **o spełnianiu warunków udziału** w postępowaniu o udzielenie zamówienia pn.: ***„Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko."***

Gmina Miastko
ul. Grunwaldzka 1
77-200 Miastko

Wykonawca:

.....

.....

(pełna nazwa)

reprezentowany przez

……....

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Adres/siedziba……

NIP……

REGON……

(w przypadku składania oferty przez podmioty występujące wspólnie podać nazwy (firmy) i dokładne adresy wszystkich członków konsorcjum)

Na potrzeby niniejszego postępowania, oświadczam, co następuje:

1. **Informacja dotycząca wykonawcy**

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez Zamawiającego w Rozdziale …… Specyfikacji Warunków Zamówienia.

2. **Informacja w związku z poleganiem na zasobach innych podmiotów**

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w Rozdziale … Specyfikacji Warunków Zamówienia, polegam na zasobach następującego/ych podmiotu/ów:

1. ……...……...……

   ……..……..……

   w następującym zakresie:

   …….

   (wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu)

2. ……...……...……

   ……..……..……..……

   w następującym zakresie: …….

(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu)

3. ……...……...……

……..……..……

w następującym zakresie: …….

(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu)

3. **Oświadczenie dotyczące podanych informacji**

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

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

(podpis wykonawcy lub osób uprawnionych do występowania w jego imieniu)

Załącznik nr 5

Oświadczenie Wykonawcy

o braku przynależności do tej samej grupy kapitałowej, w zakresie art. 108 ust. 1 pkt 5 Pzp,w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2024 r. poz. 594 z późn. zm.) w postępowaniu o udzielenie zamówienia pn.: ***„Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko."***

Gmina Miastko
ul. Grunwaldzka 1
77-200 Miastko

Wykonawca:

.....

.....

(pełna nazwa wykonawcy)

reprezentowany przez

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

Adres……

NIP……

REGON……

(w przypadku składania oferty przez Wykonawców występujących wspólnie – każdy z uczestników składa odrębne oświadczenie podając swoją nazwę (firmę) i adres)

W celu wykazania braku podstaw wykluczenia z postępowania na podstawie art. 108 ust. 1 pkt 5 Pzp,

Oświadczam, że* - w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2024 r. poz. 594 z późn. zm.).**:**

- ☐ **nie należę** (nie należymy) do tej samej grupy kapitałowej,
- ☐ **należę** (należymy) do tej samej grupy kapitałowej:

  ……

  ……..……..
  (wymienić podmioty wchodzące w skład tej samej grupy kapitałowej podając ich nazwę (firmę) i adres)

oraz składam wraz z oświadczeniem dokumenty bądź informacje potwierdzające, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu.

* zaznaczyć odpowiednie

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

(podpis wykonawcy lub osób uprawnionych do występowania w jego imieniu)

Załącznik nr 6

Oświadczenie podmiotu/ów

udostępniającego/ch zasoby, na których może polegać Wykonawca w zakresie zdolności technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej, w celu potwierdzenia spełniania warunków udziału w postępowaniu – składane na podstawie art. 125 ust. 5 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych,

o braku podstaw wykluczenia oraz spełnianiu warunków udziału

z uwzględnieniem przesłanek na podstawie art.7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego z postępowania o udzielenie zamówienia pn.: ***„Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko."***

Gmina Miastko
ul. Grunwaldzka 1
77-200 Miastko

Nazwa Podmiotu:

.....

.....

(pełna nazwa)

reprezentowany przez

……....

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Adres……

NIP……

REGON……

Na potrzeby niniejszego postępowania, **oświadczam, że:**

1) nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 Pzp oraz spełniam warunki udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuję się na udostępnione przeze mnie zasoby:

2) nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

.

……*(miejscowość),* dnia ……..…… r. ……

(podpis podmiotu udostępniającego zasoby lub osób uprawnionych do występowania w jego imieniu

Załącznik nr 7

Zobowiązanie Podmiotu

udostępniającego zasoby, do oddania do dyspozycji Wykonawcy, niezbędnych zasobów na potrzeby realizacji zamówienia - składane na podstawie art. 118 ust. 3 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych, w postępowaniu o udzielenie zamówienia publicznego pn.: ***„Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko."***

Ja/My niżej podpisani:

…….....

(imię i nazwisko osoby/ób upoważnionej/ych do reprezentowania Podmiotu udostępniającego zasoby – zgodnie z zasadami reprezentacji Podmiotu składającego zobowiązanie)

, który występowania w jego imieniu)nazwa (podpis podmiotu udostępniającego zasoby lub osób uprawnionych do występowania w jego imieniu)nazwa (firma) i dokładny adres Podmiotu oddającego Wykonawcy do dyspozycji zasoby na zasadach określonych w art. 118 Pzp)

działając w imieniu i na rzecz:

…….....

(nazwa (firma) i dokładny adres Podmiotu oddającego Wykonawcy do dyspozycji zasoby na zasadach określonych w art. 118 Pzp)

zobowiązuję/my się oddać do dyspozycji uczestniczącemu w niniejszym postępowaniu Wykonawcy:

…….....

……

(nazwa (firma) i dokładny adres Wykonawcy, który polega na zasobach ww. podmiotu na zasadach określonych w art. 118 Pzp)

następujące niezbędne zasoby na potrzeby realizacji ww. zamówienia:

…….....……

(określenie zasobu, np. wiedza i doświadczenie, potencjał techniczny, potencjał kadrowy, potencjał ekonomiczno-finansowy)

Sposób wykorzystania udostępnionych przeze mnie zasobów będzie następujący:

…….....…….....

Charakter stosunku łączącego mnie z Wykonawca będzie następujący:

…….....

Zakres mojego udziału przy wykonywaniu zamówienia będzie następujący:

…….....

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

(podpis/y Podmiotu udostępniającego zasoby lub osoby/ób uprawnionych do występowania w jego imieniu)

Załącznik nr 8

Wykaz dostaw

wykonanych w okresie 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie wraz z podaniem ich przedmiotu, dat wykonania i podmiotów, na rzecz których wykonywane zostały dostawy oraz załączenie dowodów czy te dostawy zostały wykonane należycie.

Na potrzeby postępowania o udzielenie zamówienia publicznego w trybie podstawowym na wykonanie zamówienia pn.***„ Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko."*** przedkładam niniejszy wykaz dostaw wykonanych w okresie 3 lat przed upłynięciem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy- w tym okresie wraz z podaniem ich przedmiotu, dat wykonania i podmiotów, na rzecz których wykonywane zostały dostawy oraz załączenie dowodów czy te dostawy zostały wykonane należycie.

UWAGA: Wykonawca jest zobowiązany wypełnić wszystkie rubryki, podając kompletne i jednoznaczne informacje, z których wynikać będzie spełnienie warunku w opisanego w rozdziale XIV SWZ. Wskazana dostawa dotyczy jednego wykonanego kontraktu (wynika z jednostkowej umowy zawartej z danym podmiotem). Jeżeli w ofercie zostanie wskazana więcej niż jedna część zamówienia wówczas wartość dostaw nie może być niższa niż suma wymaganych wartości dostaw dla wszystkich części wskazanych w ofercie.

Rodzaj dostaw	Wartość dostaw brutto	Daty wykonania od – do	Miejsce wykonania	Podmiot na rzecz, którego dostawy te zostały wykonane

Wraz z wykazem należy załączyć dokument/dowody potwierdzające, że wymienione w wykazie dostawy została lub jest wykonywana należycie.

Dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy:

……
Podpis wykonawcy lub osoby upoważnionej do występowania w jego imieniu

Załącznik nr 9

Wykaz osób skierowanych do realizacji zamówienia

w postępowaniu o udzielenie zamówienia publicznego o wartości mniejszej niż progi unijne określone w przepisach wydanych na podstawie art. 3 ust. 3 Pzp, prowadzonym w trybie podstawowym, o którym mowa w art. 275 pkt 1 Pzp pn.: ***„ Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko."***

Gmina Miastko
ul. Grunwaldzka 1
77-200 Miastko

Składając ofertę w przedmiotowym postepowaniu oświadczam, że dysponuję osobą posiadającą doświadczenie zawodowe gwarantujące należyte wykonanie zamówienia w zakresie niezbędnym do wykazania spełnienia warunku - określonego w Rozdziale XIV swz:

Imię i nazwisko	Doświadczenie zawodowe w latach	Nazwa przeprowadzonej usługi szkoleniowej/ zakres	Termin przeprowadzonej usługi szkoleniowej	Podmiot, na rzecz którego usługi zostały wykonane (nazwa i adres)

Wraz z wykazem należy załączyć dokument/dowody potwierdzające, że wymienione w wykazie osoby posiadają odpowiednie kwalifikacje oraz ze usługi przeprowadzenia wystąpień/szkoleń/prelekcje związanych z tematyką bezpieczeństwa informacji wykonywana należycie.

Dowodami, o których mowa są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi zostały wykonane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy

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

(podpis/y Podmiotu udostępniającego zasoby lub osoby/ób uprawnionych do występowania w jego imieniu)

Załącznik nr 10

UMOWA nr ……/ WOA.272….2024.MM (wzór)
O WYKONANIE DOSTAWY cz. I

W dniu ……..2024 r. w Miastku pomiędzy Gminą Miastko reprezentowaną przez Burmistrza Miastka - Jerzego Wójtowicza, mającą swą siedzibę w Miastku przy ul. Grunwaldzkiej 1, zwaną w dalszej części umowy „Zamawiającym",
a
……
zwanym w dalszej części umowy „Wykonawcą" w imieniu, którego działa:
…….….
w rezultacie dokonania przez Zamawiającego wyboru oferty Wykonawcy w trybie podstawowym na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320) została zawarta umowa o następującej treści:

§1.

1. Przedmiotem umowy jest rozbudowa infrastruktury informatycznej urzędu oparta na dostawie sprzętu wraz z instalacją, montażem i przeniesieniem danych z obecnej sieci informatycznej oraz wdrożenie oprogramowania do zarządzania siecią IT wraz z konfiguracją sieci VLAN. Wykonawca jest zobowiązany do sporządzenia dokumentacji z przeprowadzonego wdrożenia oraz przeprowadzenia szkoleń specjalistycznych z zastosowanych rozwiązań, zgodnie z opisem przedmiotu zamówienia udostępnionym w postępowaniu przez Zamawiającego (dalej: „OPZ").
2. Parametry sprzętu informatycznego i oprogramowania, oraz zasady wdrożenia określa OPZ – załącznik nr 1 do specyfikacji warunków zamówienia (swz).
3. Wykonawca jest zobligowany do powołania i przedstawienia, przed jego przystąpieniem do pracy, zespołu wdrożeniowego, w którego skład będzie wchodził kierownik zespołu.
4. Osoby wchodzące w skład zespołu wdrożeniowego :
   1) ……..- kierownik zespołu;
   2) ……;
   3) ……
5. Osoby odpowiedzialne za realizację Umowy:
   1) ze strony Zamawiającego: Marcin Woszczak: : informatyk@um.miastko.pl., tel.598570779.
   2) ze strony Wykonawcy …….
6. Przedmiot zamówienia jest dofinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02.-CS.01-001/23. Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/2110/FERC.02.02-CS.01-001/23/2024.

§ 2.

Wykonawca zobowiązuje się wykonać przedmiot zamówienia w terminie 90 dni od dnia podpisania umowy.

§ 3.

1. Wykonawca w terminie 14 dni od dnia zawarcia umowy przedstawi Zamawiającemu harmonogram realizacji prac wdrożeniowych (zwany dalej: „harmonogramem"). Harmonogram podlega zatwierdzeniu przez Zamawiającego.
2. Wykonawca w harmonogramie wdrożenia musi uwzględnić w szczególności podział na zadania, takie jak: projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.
3. Wykonawca umożliwi Zamawiającemu udział we wszystkich pracach (zadaniach) realizowanych przez Wykonawcę w ramach realizacji przedmiotu zamówienia.
4. Zamawiający na etapie wdrożenia rozbudowy infrastruktury sieci informatycznej będzie dokonywał częściowych odbiorów zgodnie z harmonogramem.
5. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca przeprowadzi zgodnie z zapisami OPZ w uzgodnieniu z Zamawiającym, zgodnie z obowiązującymi przepisami oraz zasadami technicznymi wykonywania projektów informatycznych.

§ 4.

1. Po wykonaniu zamówienia zostanie przeprowadzony odbiór końcowy przedmiotu zamówienia.

2. Zamawiający wyznaczy termin odbioru końcowego niezwłocznie, lecz nie później niż w ciągu 7 dni od dnia zgłoszenia przez Wykonawcę gotowości do przeprowadzenia odbioru końcowego.
3. Warunkiem dokonania odbioru końcowego jest dostarczenie przez Wykonawcę dokumentacji powykonawczej, obejmującej dokumentację użytkową, techniczną i eksploatacyjną. Dokumentacja powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej i papierowej.
4. W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań. Powinna zawierać następujące elementy:
   1) schemat infrastruktury i architekturę rozwiązania wraz z opisem;
   2) zasady licencjonowania dostarczonych elementów;
   3) konfigurację sprzętową i logiczną elementów infrastruktury dla wdrożonych systemów;
   4) procedury uruchamiania i zatrzymywania wdrożonych systemów oraz elementów infrastruktury;
   5) procedury konfiguracji kont w dostarczonych systemach;
   6) procedury awaryjne umożliwiające dostęp do infrastruktury w przypadku awarii;
   7) procedury wykonywania odtworzenia wdrożonych systemów z kopii zapasowej;
   8) procedury opisujące standardowe działania administracyjne;
   9) procedury odzyskania wdrożonych systemów po awarii;
   10) wytyczne (dobre praktyki) dla administratorów;
   11) spis dokumentacji zewnętrznej do której odwołuje się dokumentacja powykonawcza.
5. Jeżeli w toku czynności odbiorowych zostaną stwierdzone wady, Wykonawca zobowiązany będzie do ich usunięcia. W takiej sytuacji Zamawiający wyznaczy dodatkowy terminu odbioru.
6. Z czynności odbioru końcowego spisany zostanie protokół zawierający wszelkie ustalenia dokonane w toku odbioru.
7. Protokół odbioru podpisany przez strony stanowi podstawę wystawienia faktury za wykonanie całości zamówienia.

§ 5.

1. Wynagrodzenie Wykonawcy za wykonanie zamówienia wynosi …..... zł brutto (słownie: .....), w tym wartość VAT: …… zł (jeżeli dotyczy), wynagrodzenie netto: …….. zł.
2. Zapłata wynagrodzenia nastąpi z zachowaniem 30-dniowego terminu płatności.
3. Wynagrodzenie, o którym mowa w ust.1 obejmuje wszystkie koszty związane z realizacja zamówienia.
4. Zapłata wynagrodzenia zostanie dokonana na podstawie wystawionej przez Wykonawcę faktury VAT lub rachunku w złotych polskich.
5. Zmiana wierzyciela z tytułu przysługującego Wykonawcy wynagrodzenia wymaga zgody Zamawiającego, wyrażonej w formie pisemnej pod rygorem nieważności.

§ 6.

1. Wykonawca udziela Zamawiającemu gwarancji na sprzęt będący przedmiotem umowy – zgodnie z warunkami przedstawionymi w OPZ stanowiącymi integralną część umowy.
2. Okres gwarancji, o którym mowa w ust. 1 rozpoczyna się z dniem podpisania protokołu, o którym mowa w § 4 ust. 6.
3. W trakcie trwania gwarancji Zamawiający lub podmiot przez niego upoważniony uprawniony jest do dokonywania przeglądów gwarancyjnych przedmiotu umowy. O przeglądzie gwarancyjnym Zamawiający lub podmiot przez niego upoważniony, powiadamia Wykonawcę. Nieobecność Wykonawcy na przeglądzie gwarancyjnym nie wstrzymuje przeprowadzenia przeglądu i nie stanowi przeszkody do jego skutecznego dokonania, a Zamawiający jest wówczas zobowiązany przesłać Wykonawcy protokół przeglądu gwarancyjnego wraz z wezwaniem do usunięcia stwierdzonych wad (jeżeli takie wystąpią) w określonym przez Zamawiającego terminie, wynoszącym co najmniej 14 dni.
4. Wykonawca, niezależnie od gwarancji, ponosi odpowiedzialność z tytułu rękojmi za wady fizyczne oraz wady prawne sprzętu zgodnie z kodeksem cywilnym.
5. Zamawiający będzie dokonywał zgłoszeń w zakresie gwarancji, rękojmi oraz specjalistycznego wsparcia IT w zakresie cyberbezpieczeństwa, Wykonawcy na adres e-mail ……. lub telefonicznie …….. w dni robocze w godz. 7:30-15:00.
6. Wykonawca zapewni bezpłatne usunięcie awarii w okresie trwania gwarancji.
7. W przypadku stwierdzenia wady ukrytej sprzętu Wykonawca zobowiązany jest do jego wymiany na nowy wolny od wad zgodnie z warunkami przedstawionymi w OPZ oraz ofercie.

8. Wykonawca ponosi wszelkie koszty związane w wykonaniem obowiązków wynikających z gwarancji.
9. Wykonawca zobowiązuje się do zapewnienia kontynuacji świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) w przypadku niemożliwości ich wypełnienia przez Wykonawcę.
10. Jeżeli Wykonawca nie usunie wad ujawnionych w okresie gwarancji w określonym przez Zamawiającego terminie, uwzględniającym możliwości techniczne lub technologiczne dotyczące usunięcia wady, Zamawiający, po uprzednim zawiadomieniu Wykonawcy, jest uprawniony do zlecenia usunięcia wad podmiotowi trzeciemu na koszt i ryzyko Wykonawcy.

§ 8.

1. Wykonawca zapłaci Zamawiającemu kary umowne:
   1) za zwłokę w wykonaniu zamówienia w stosunku do terminu, o którym mowa w § 2 - w wysokości 0,1% wynagrodzenia brutto za każdy rozpoczęty dzień kalendarzowy zwłoki, jaki upłynie pomiędzy terminem, o którym mowa w § 2 a faktycznym dniem wykonania zamówienia;
   2) za zwłokę Wykonawcy w usunięciu wad stwierdzonych przy podczas przeglądu gwarancyjnego lub odbioru ostatecznego - w wysokości 0,1% wynagrodzenia brutto za każdy rozpoczęty dzień kalendarzowy zwłoki liczony od dnia upływu terminu na usunięcie wad.
2. Limit kar umownych, jakich Zamawiający może żądać od Wykonawcy ze wszystkich tytułów przewidzianych w niniejszej umowie wynosi 20% wynagrodzenia brutto za wykonanie całości zamówienia.
3. Jeżeli kara umowna z któregokolwiek tytułu wymienionego w ust. 1 nie pokrywa poniesionej szkody, to Zamawiający może dochodzić odszkodowania uzupełniającego na zasadach ogólnych określonych w ustawie z 23 kwietnia 1964 r. – Kodeks cywilny.
4. Kara umowna z tytułu zwłoki przysługuje za każdy rozpoczęty dzień kalendarzowy zwłoki i jest wymagalna od dnia następnego po upływie terminu jej zapłaty. Termin zapłaty kary umownej wynosi 14 dni kalendarzowych od dnia skutecznego doręczenia Wykonawcy wezwania do zapłaty. W razie zwłoki z zapłatą kary umownej Zamawiający może żądać odsetek ustawowych za każdy dzień kalendarzowy opóźnienia.

§ 9.

1. Zamawiającemu przysługuje prawo odstąpienia od umowy, gdy:
   1) Wykonawca pozostaje w zwłoce w terminie wykonania przedmiotu umowy, który został określony w § 2 więcej niż 7 dni – w terminie 14 dni od dnia powzięcia przez Zamawiającego informacji o upływie 7-dniowego terminu zwłoki w realizacji dostawy sprzętu;
   2) Wykonawca nie realizuje zamówienia zgodnie z umową lub też nienależycie wykonuje swoje zobowiązania umowne i pomimo pisemnego lub przesłanego drogą elektroniczną wezwania otrzymanego od Zamawiającego nie przystąpił do realizacji umowy zgodnie z jej warunkami w terminie 14 dni od dnia stwierdzenia przez Zamawiającego danej okoliczności;
   3) w terminie 30 dni od dnia powzięcia wiadomości o zaistnieniu istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, lub dalsze wykonywanie umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu.
2. Wykonawcy przysługuje prawo odstąpienia od umowy, gdy Zamawiający odmawia bez wskazania uzasadnionej przyczyny odbioru dostarczonego sprzętu i pomimo pisemnego lub przesłanego drogą elektroniczną wezwania nie przystąpił do czynności odbioru w terminie 7 dni od dnia upływu terminu wyznaczonego przez Wykonawcę w wezwaniu na przystąpienie przez Zamawiającego do odbioru dostarczonego sprzętu.
3. Odstąpienie od umowy, o którym jest mowa w ust. 1 i 2 powinno nastąpić w formie pisemnej pod rygorem nieważności takiego oświadczenia i winno zawierać uzasadnienie.
4. Zamawiający zastrzega sobie prawo do rozwiązania niniejszej umowy, gdy Wykonawca nie wywiązuje się w sposób właściwy ze zobowiązań ciążących na nim z mocy postanowień umowy, po uprzednim pisemnym wezwaniu Wykonawcy do zaprzestania naruszeń umowy oraz usunięcia skutków naruszeń uprzednio zaistniałych i bezskutecznym upływie jednostronnie wyznaczonego odpowiedniego terminu ich usunięcia.
5. W przypadku powzięcia przez Strony informacji o braku możliwości realizacji umowy bez szkód dla Zamawiającego lub Wykonawcy, Strony mogą rozwiązać umowę za porozumieniem stron rozliczając zrealizowaną część zamówienia na zasadach określonych w umowie.
6. Rozwiązanie Umowy, o którym mowa ust. 4 i 5 następuje w formie pisemnej pod rygorem nieważności.

§ 10.

1. Wszelkie zmiany niniejszej umowy wymagają dla swej ważności formy pisemnej pod rygorem nieważności i będą dopuszczalne w granicach unormowania art. 455 ustawy Prawo zamówień publicznych.
2. Zamawiający dopuszcza możliwość zmiany ustaleń zawartej umowy, w stosunku do treści oferty Wykonawcy, w następującym zakresie i okolicznościach:
   1) zmiany warunków realizacji i zakresu przedmiotowego umowy niezbędne do prawidłowej realizacji zamówienia związane z:
   a) koniecznością zrealizowania przedmiotu umowy przy zastosowaniu innych rozwiązań niż wskazane w Opisie Przedmiotu Zamówienia w sytuacji, gdyby zastosowanie przewidzianych rozwiązań groziłoby niewykonaniem lub wadliwym wykonaniem przedmiotu umowy,
   b) koniecznością zrealizowania przedmiotu umowy przy zastosowaniu innych rozwiązań ze względu na zmiany obowiązującego prawa,
   c) wprowadzeniem nowych rozwiązań technicznych z uwagi na postęp technologiczny, jeżeli zmiana ta jest korzystna dla Zamawiającego,
   d) wystąpieniem okoliczności powodujących, że niemożliwe jest zrealizowanie przedmiotu umowy w sposób określony w SWZ i złożonej ofercie, które nie były możliwe do przewidzenia w momencie zawarcia umowy,
   2) zmiany producenta lub modelu/typu sprzętu, wersji oprogramowania (zastąpienie produktu /dalej: sprzętu/wyposażenia/oprogramowania/ lub rozszerzenie produktu o produkt równoważny lub wyższej jakości) w przypadku:
   a) zaprzestania produkcji sprzętu/wyposażenia/oprogramowania objętego umową, w tym czasowego wstrzymania produkcji, pod warunkiem, iż odpowiednik jest tej samej lub wyższej jakości, za cenę nie wyższą niż cena produktu objętego umową,
   b) wprowadzenia do sprzedaży przez producenta zmodyfikowanego/udoskonalonego produktu, za cenę nie wyższą niż cena produktu objętego umową,
   c) zmiany numeru katalogowego produktu, nazwy produktu, przy zachowaniu jego parametrów,
   3) zmiany terminu wykonania przedmiotu umowy o czas zwłoki, jeżeli taka zwłoka jest lub będzie miała wpływ na wykonanie przedmiotu umowy w następujących przypadkach:
   a) zwłoki związanej z czynnościami Zamawiającego, od których uzależniona jest możliwość wykonania obowiązków nałożonych umową na Wykonawcę,
   b) zawieszenia terminu realizacji zamówienia przez Zamawiającego, z przyczyn od niego niezależnych, c) określonych w ust. 2 pkt 1, 2 i 5 umowy - termin wykonania umowy może ulec zmianie o czas, o jaki wyżej wskazane okoliczności wpłynęły na termin wykonania umowy przez Wykonawcę, to jest uniemożliwiły Wykonawcy terminową realizację przedmiotu umowy,
   5) zmiany w zakresie podwykonawców wskazanych w ofercie, pod warunkiem wyrażenia zgody Zamawiającego na taką zmianę,
   6) wystąpienia siły wyższej (rozumianej jako zdarzenie zewnętrzne, niemożliwe do przewidzenia, którego skutkom nie można zapobiec, w szczególności: powódź, pożar, trzęsienie ziemi, epidemia, zamieszki, strajki, działania zbrojne, zakaz przemieszczania się, blokady) uniemożliwiającej wykonanie przedmiotu umowy zgodnie z jej postanowieniami.
   7) w razie zmiany wysokości stawki VAT Strony dokonują zmiany uwzględniającej nową wysokość tej stawki,
   8) zmian wynikających z przepisów prawa,
   9) rezygnacji przez Zamawiającego z realizacji części przedmiotu umowy; w takim przypadku wynagrodzenie przysługujące Wykonawcy zostanie pomniejszone, przy czym Zamawiający zapłaci za wszystkie prawidłowo zrealizowane dostawy.
3. Jeżeli na wskutek okoliczności, o których mowa w art. 455 ust. 1 pkt 1, 3, 4 i ust. 2 ustawy Prawo zamówień publicznych, zachodzi konieczność zmiany wynagrodzenia, Wykonawca przedłoży do akceptacji Zamawiającego kalkulację ceny jednostkowej sprzętu z uwzględnieniem cen z formularza ofertowego.
4. Powiadomienie o konieczności wprowadzenia zmian w zawartej umowie nie może nastąpić później niż 3 dni od zaistnienia okoliczności uzasadniających zmiany w umowie.
5. Warunkiem dokonania zmian, o których mowa w ust. 2 i 3, jest złożenie uzasadnionego wniosku przez stronę inicjującą zmianę, określającego przyczyny i zakres zmiany oraz potwierdzającego wystąpienie okoliczności wymienionych w ust. 2 i 3 oraz wyrażenie zgody przez drugą stronę umowy.

§ 11.

1. Wykonawca zobowiązuje się do bezwzględnego zachowania w poufności wszelkich informacji uzyskanych w związku z wykonywaniem Umowy.
2. Przez obowiązek, o jakim mowa w ust. 1 powyżej rozumie się w szczególności zakaz:
   1) zapoznawania się przez Wykonawcę z dokumentami, analizami, zawartością dysków twardych i innych nośników informacji itp.- nie związanymi ze zleconym zakresem prac;
   2) zabierania, kopiowania oraz powielania dokumentów i danych, a w szczególności udostępniania ich osobom trzecim;
   3) informowania osób trzecich o danych objętych nakazem poufności.
3. Za osobę trzecią uważa się osoby nie wymienione w § 1 ust. 5 , którego zmianę Strony dopuszczają w drodze wymiany pism.
4. Wykonawca zobowiązuje się zapoznać i przestrzegać aktów regulujących zasady postępowania z dokumentami lub danymi w zakresie niezbędnym do realizacji Umowy, które obowiązują Zamawiającego.
5. Wykonawca zobowiązuje się informować przedstawicieli Zamawiającego o wszystkich zauważonych nieprawidłowościach mogących mieć wpływ na bezpieczeństwo informacji.

§ 12.

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcom.
2. Wykonawca zobowiązuje się do wykonania przedmiotu umowy własnymi siłami/Wykonawca powierzy następującym podwykonawcom następującą część zamówienia:* (*niepotrzebne skreślić).
   1) Podwykonawca: ....., część zamówienia: .....,
   2) Podwykonawca: ....., część zamówienia: .....
3. Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia.
4. Wykonawca ponosi odpowiedzialność za działania lub zaniechanie działań podwykonawców tak jak za działania lub zaniechania własne.
5. Umowa o podwykonawstwo nie może zawierać postanowień kształtujących prawa i obowiązki podwykonawcy, w zakresie kar umownych oraz postanowień dotyczących warunków wypłaty wynagrodzenia, w sposób dla niego mniej korzystny niż prawa i obowiązki Wykonawcy, ukształtowane postanowieniami niniejszej umowy.

§ 13.

1. Wszelkie zmiany niniejszej Umowy wymagają dla swej ważności zachowania formy pisemnej.
2. W sprawach nieuregulowanych niniejszą Umową zastosowanie znajdują przepisy prawa powszechnie obowiązującego, w tym kodeksu cywilnego.
3. Wszelkie spory wynikłe między Stronami związane z zawarciem lub wykonaniem niniejszej Umowy Strony zobowiązują się rozstrzygać w drodze przyjaznych negocjacji. W przypadku braku porozumienia, Strony zgodnie poddają ewentualne spory pod rozstrzygnięcie właściwego miejscowo sądu powszechnego.

§ 14.

Załącznikami do umowy są:
1) harmonogram rzeczowo-finansowy;
2) specyfikacja warunków zamówienia wraz z załącznikami;
3) oferta Wykonawcy wraz z załącznikami;
4) *umowa regulującą współpracę wykonawców wspólnie ubiegających się o udzielenie zamówienia – jeżeli dotyczy.*

§ 15.

4. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, jeden dla Wykonawcy, dwa dla Zamawiającego.

ZAMAWIAJĄCY WYKONAWCA

UMOWA nr ……/ WOA.272….2024.MM (wzór)
O WYKONANIE DOSTAWY cz. II

W dniu ……..2024 r. w Miastku pomiędzy Gminą Miastko reprezentowaną przez Burmistrza Miastka - Jerzego Wójtowicza, mającą swą siedzibę w Miastku przy ul. Grunwaldzkiej 1, zwaną w dalszej części umowy „Zamawiającym",
a
……
zwanym w dalszej części umowy „Wykonawcą" w imieniu, którego działa:
……..….
w rezultacie dokonania przez Zamawiającego wyboru oferty Wykonawcy w trybie podstawowym na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320) została zawarta umowa o następującej treści:

§1.

1. Przedmiotem umowy jest dostawa oprogramowania do monitorowania infrastruktury sieci informatycznej i urządzeń dla jednostki podległej oraz dostawę usług chmurowych w ramach zabezpieczenia poczty i stron internetowych Gminy, zgodnie z opisem przedmiotu zamówienia udostępnionym w postępowaniu przez Zamawiającego (dalej: „OPZ").
2. Parametry sprzętu informatycznego i oprogramowania, oraz zasady wdrożenia określa OPZ – załącznik nr 1 do specyfikacji warunków zamówienia (swz).
3. Przedmiot zamówienia jest dofinansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02.-CS.01-001/23. Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/2110/FERC.02.02-CS.01-001/23/2024.
4. Osoby odpowiedzialne za realizację Umowy:
   1) ze strony Zamawiającego : Marcin Woszczak, informatyk@miastko.pl, tel.598570779
   2) ze strony Wykonawcy …….

§ 2.

Wykonawca zobowiązuje się wykonać przedmiot zamówienie w terminie 30 dni od dnia podpisania umowy.

§ 3.

1. Po wykonaniu zamówienia zostanie przeprowadzony odbiór końcowy przedmiotu zamówienia.
2. Warunkiem dokonania odbioru końcowego jest dostarczenie przez Wykonawcę dokumentacji powykonawczej obejmującej dokumentację użytkową, techniczną i eksploatacyjną.
3. Protokół odbioru podpisany przez strony stanowi podstawę wystawienia faktury za wykonanie całości zamówienia.

§ 4.

1. Wynagrodzenie Wykonawcy za wykonanie zamówienia wynosi **…..... zł brutto (słownie: .....)**, w tym wartość VAT: …… zł (jeżeli dotyczy), wynagrodzenie netto: …….. zł.
2. Zapłata wynagrodzenia nastąpi z zachowaniem 30 dniowego terminu płatności.
3. Wynagrodzenie, o którym mowa w ust.1 obejmuje wszystkie koszty związane z realizacja zamówienia.
4. Zapłata wynagrodzenia zostanie dokonana na podstawie wystawionej przez Wykonawcę faktury VAT lub rachunku w złotych polskich.
5. Zmiana wierzyciela z tytułu przysługującego Wykonawcy wynagrodzenia wymaga zgody Zamawiającego, wyrażonej w formie pisemnej pod rygorem nieważności.

§ 5.

1. Wykonawca oświadcza, że zaoferowane w Ofercie urządzenia są objęte gwarancją producenta oraz Wykonawcy przez okres wskazany w Ofercie, oraz wsparciem Wykonawcy na warunkach określonych w OPZ, od dnia podpisania protokołu odbioru, o którym mowa w § 3 ust. 3.

2. W przypadku odmowy świadczenia usług z tytułu gwarancji producenta na warunkach ujętych w OPZ lub świadczenia gwarancji na innych warunkach, obowiązki z tytułu gwarancji przechodzą na Wykonawcę, który jest obowiązany świadczyć z tego tytułu w miejsce producenta usługi na warunkach nie gorszych niż ujęte w OPZ i w ramach wynagrodzenia określonego w § 4 ust. 1.
3. Uprawnienia wynikające z udzielonej gwarancji nie wyłączają możliwości dochodzenia przez Zamawiającego uprawnień z tytułu rękojmi za wady.

§ 6.

1. Wykonawca zapłaci Zamawiającemu kary umowne:
   1) za zwłokę w wykonaniu zamówienia w stosunku do terminu, o którym mowa w § 2 - w wysokości 0,1 % wynagrodzenia brutto za każdy rozpoczęty dzień kalendarzowy zwłoki, jaki upłynie pomiędzy terminem, o którym mowa w § 2 a faktycznym dniem wykonania zamówienia;
   2) za zwłokę Wykonawcy w usunięciu wad stwierdzonych przy podczas przeglądu gwarancyjnego lub odbioru ostatecznego - w wysokości 0,1 % wynagrodzenia brutto za każdy rozpoczęty dzień kalendarzowy zwłoki liczony od dnia upływu terminu na usunięcie wad.
2. Limit kar umownych, jakich Zamawiający może żądać od Wykonawcy ze wszystkich tytułów przewidzianych w niniejszej umowie wynosi 20 % wynagrodzenia brutto za wykonanie całości zamówienia.
3. Jeżeli kara umowna z któregokolwiek tytułu wymienionego w ust. 1 nie pokrywa poniesionej szkody, to Zamawiający może dochodzić odszkodowania uzupełniającego na zasadach ogólnych określonych w ustawie z 23 kwietnia 1964 r. – Kodeks cywilny.
4. Kara umowna z tytułu zwłoki przysługuje za każdy rozpoczęty dzień kalendarzowy zwłoki i jest wymagalna od dnia następnego po upływie terminu jej zapłaty. Termin zapłaty kary umownej wynosi 14 dni kalendarzowych od dnia skutecznego doręczenia Wykonawcy wezwania do zapłaty. W razie zwłoki z zapłatą kary umownej Zamawiający może żądać odsetek ustawowych za każdy dzień kalendarzowy opóźnienia.

§ 7.

1. Zamawiającemu przysługuje prawo odstąpienia od umowy, gdy:
   1) Wykonawca pozostaje w zwłoce w terminie wykonania przedmiotu umowy, który został określony w § 2 więcej niż 7 dni – w terminie 14 dni od dnia powzięcia przez Zamawiającego informacji o upływie 7-dniowego terminu zwłoki w realizacji dostawy sprzętu;
   2) Wykonawca nie realizuje zamówienia zgodnie z umową lub też nienależycie wykonuje swoje zobowiązania umowne i pomimo pisemnego lub przesłanego drogą elektroniczną wezwania otrzymanego od Zamawiającego nie przystąpił do realizacji umowy zgodnie z jej warunkami w terminie 14 dni od dnia stwierdzenia przez Zamawiającego danej okoliczności;
   3) w terminie 30 dni od dnia powzięcia wiadomości o zaistnieniu istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, lub dalsze wykonywanie umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu.
2. Wykonawcy przysługuje prawo odstąpienia od umowy, gdy Zamawiający odmawia bez wskazania uzasadnionej przyczyny odbioru dostarczonego sprzętu i pomimo pisemnego lub przesłanego drogą elektroniczną wezwania nie przystąpił do czynności odbioru w terminie 7 dni od dnia upływu terminu wyznaczonego przez Wykonawcę w wezwaniu na przystąpienie przez Zamawiającego do odbioru dostarczonego sprzętu.
3. Odstąpienie od umowy, o którym jest mowa w ust. 1 i 2 powinno nastąpić w formie pisemnej pod rygorem nieważności takiego oświadczenia i winno zawierać uzasadnienie.
4. Zamawiający zastrzega sobie prawo do rozwiązania niniejszej umowy, gdy Wykonawca nie wywiązuje się w sposób właściwy ze zobowiązań ciążących na nim z mocy postanowień umowy, po uprzednim pisemnym wezwaniu Wykonawcy do zaprzestania naruszeń umowy oraz usunięcia skutków naruszeń uprzednio zaistniałych i bezskutecznym upływie jednostronnie wyznaczonego odpowiedniego terminu ich usunięcia.
5. W przypadku powzięcia przez Strony informacji o braku możliwości realizacji umowy bez szkód dla Zamawiającego lub Wykonawcy, Strony mogą rozwiązać umowę za porozumieniem stron rozliczając zrealizowaną część zamówienia na zasadach określonych w umowie.
6. Rozwiązanie Umowy, o którym mowa ust. 4 i 5 następuje w formie pisemnej pod rygorem nieważności.

§ 8.

1. Wszelkie zmiany niniejszej umowy wymagają dla swej ważności formy pisemnej pod rygorem nieważności i będą dopuszczalne w granicach unormowania art. 455 ustawy Prawo zamówień publicznych.
2. Zamawiający dopuszcza możliwość zmiany ustaleń zawartej umowy, w stosunku do treści oferty Wykonawcy, w następującym zakresie i okolicznościach:
   1) zmiany warunków realizacji i zakresu przedmiotowego umowy niezbędne do prawidłowej realizacji zamówienia związane z:
      a) koniecznością zrealizowania przedmiotu umowy przy zastosowaniu innych rozwiązań niż wskazane w Opisie Przedmiotu Zamówienia w sytuacji, gdyby zastosowanie przewidzianych rozwiązań groziłoby niewykonaniem lub wadliwym wykonaniem przedmiotu umowy,
      b) koniecznością zrealizowania przedmiotu umowy przy zastosowaniu innych rozwiązań ze względu na zmiany obowiązującego prawa,
      c) wprowadzeniem nowych rozwiązań technicznych z uwagi na postęp technologiczny, jeżeli zmiana ta jest korzystna dla Zamawiającego,
      d) wystąpieniem okoliczności powodujących, że niemożliwe jest zrealizowanie przedmiotu umowy w sposób określony w SWZ i złożonej ofercie, które nie były możliwe do przewidzenia w momencie zawarcia umowy,
   2) zmiany producenta lub modelu/typu sprzętu, wersji oprogramowania (zastąpienie produktu /dalej: sprzętu/wyposażenia/oprogramowania/ lub rozszerzenie produktu o produkt równoważny lub wyższej jakości) w przypadku:
      a) zaprzestania produkcji sprzętu/wyposażenia/oprogramowania objętego umową, w tym czasowego wstrzymania produkcji, pod warunkiem, iż odpowiednik jest tej samej lub wyższej jakości, za cenę nie wyższą niż cena produktu objętego umową,
      b) wprowadzenia do sprzedaży przez producenta zmodyfikowanego/udoskonalonego produktu, za cenę nie wyższą niż cena produktu objętego umową,
      c) zmiany numeru katalogowego produktu, nazwy produktu, przy zachowaniu jego parametrów,
   3) zmiany terminu wykonania przedmiotu umowy o czas zwłoki, jeżeli taka zwłoka jest lub będzie miała wpływ na wykonanie przedmiotu umowy w następujących przypadkach:
      a) zwłoki związanej z czynnościami Zamawiającego, od których uzależniona jest możliwość wykonania obowiązków nałożonych umową na Wykonawcę,
      b) zawieszenia terminu realizacji zamówienia przez Zamawiającego, z przyczyn od niego niezależnych,
      c) określonych w ust. 2 pkt. 1, 2 i 5 umowy - termin wykonania umowy może ulec zmianie o czas, o jaki wyżej wskazane okoliczności wpłynęły na termin wykonania umowy przez Wykonawcę, to jest uniemożliwiły Wykonawcy terminową realizację przedmiotu umowy,
   4) zmiany w zakresie podwykonawców wskazanych w ofercie, pod warunkiem wyrażenia zgody Zamawiającego na taką zmianę,
   5) wystąpienia siły wyższej (rozumianej jako zdarzenie zewnętrzne, niemożliwe do przewidzenia, którego skutkom nie można zapobiec, w szczególności: powódź, pożar, trzęsienie ziemi, epidemia, zamieszki, strajki, działania zbrojne, zakaz przemieszczania się, blokady) uniemożliwiającej wykonanie przedmiotu umowy zgodnie z jej postanowieniami.
   6) w razie zmiany wysokości stawki VAT Strony dokonują zmiany uwzględniającej nową wysokość tej stawki,
   7) zmian wynikających z przepisów prawa,
   8) rezygnacji przez Zamawiającego z realizacji części przedmiotu umowy. W takim przypadku wynagrodzenie przysługujące Wykonawcy zostanie pomniejszone, przy czym Zamawiający zapłaci za wszystkie prawidłowo zrealizowane dostawy.
3. Jeżeli na wskutek okoliczności, o których mowa w art. 455 ust. 1 pkt. 1, 3, 4 i ust. 2 ustawy Prawo zamówień publicznych, zachodzi konieczność zmiany wynagrodzenia, Wykonawca przedłoży do akceptacji Zamawiającego kalkulację ceny jednostkowej sprzętu z uwzględnieniem cen z formularza ofertowego.
4. Powiadomienie o konieczności wprowadzenia zmian w zawartej umowie nie może nastąpić później niż 3 dni od zaistnienia okoliczności uzasadniających zmiany w umowie.
5. Warunkiem dokonania zmian, o których mowa w ust. 2 i 3, jest złożenie uzasadnionego wniosku przez stronę inicjującą zmianę, określającego przyczyny i zakres zmiany oraz potwierdzającego wystąpienie okoliczności wymienionych w ust. 2 i 3 oraz wyrażenie zgody przez drugą stronę umowy.

§ 9.

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcom.
2. Wykonawca zobowiązuje się do wykonania przedmiotu umowy własnymi siłami/Wykonawca powierzy następującym podwykonawcom następującą część zamówienia:* (*niepotrzebne skreślić).
   1) Podwykonawca: ....., część zamówienia: .....,
   2) Podwykonawca: ....., część zamówienia: .....
3. Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia.
4. Wykonawca ponosi odpowiedzialność za działania lub zaniechanie działań podwykonawców tak jak za działania lub zaniechania własne.
5. Umowa o podwykonawstwo nie może zawierać postanowień kształtujących prawa i obowiązki podwykonawcy, w zakresie kar umownych oraz postanowień dotyczących warunków wypłaty wynagrodzenia, w sposób dla niego mniej korzystny niż prawa i obowiązki Wykonawcy, ukształtowane postanowieniami niniejszej umowy.

§ 10.

1. Wszelkie zmiany niniejszej Umowy wymagają dla swej ważności zachowania formy pisemnej.
2. W sprawach nieuregulowanych niniejszą Umową zastosowanie znajdują przepisy prawa powszechnie obowiązującego, w tym kodeksu cywilnego.
3. Wszelkie spory wynikłe między Stronami związane z zawarciem lub wykonaniem niniejszej Umowy Strony zobowiązują się rozstrzygać w drodze przyjaznych negocjacji. W przypadku braku porozumienia, Strony zgodnie poddają ewentualne spory pod rozstrzygnięcie właściwego miejscowo sądu powszechnego.

§ 11.

Załącznikami do umowy są:

1) specyfikacja warunków zamówienia wraz z załącznikami;
2) oferta Wykonawcy wraz z załącznikami;
3) *umowa regulującą współpracę wykonawców wspólnie ubiegających się o udzielenie zamówienia – jeżeli dotyczy.*

§ 12.

1. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, jeden dla Wykonawcy, dwa dla Zamawiającego.

ZAMAWIAJĄCY WYKONAWCA

Załącznik nr 11

KLAUZULA INFORMACYJNA O PRZETWARZANIU DANYCH OSOBOWYCH

Realizując wymogi przepisów 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 „RODO"), uprzejmie informujemy o zasadach przetwarzania danych osobowych oraz o przysługujących prawach z tym związanych.

1. Administratorem danych osobowych przetwarzanych w Urzędzie Miejskim w Miastku jest Burmistrz Miastka (adres: ul. Grunwaldzka 1, 77-200 Miastko; telefon: +48 59 857 07 00; faks: +48 59 857 23 68; adres poczty elektronicznej: sekretariat@um.miastko.pl).
2. Pytania dotyczące sposobu i zakresu przetwarzania danych osobowych, a także przysługujących uprawnień, można kierować do Inspektora Ochrony Danych Osobowych za pomocą adresu poczty elektronicznej: iodo@um.miastko.pl
3. Pani/Pana dane osobowe przetwarzane będą na podstawie przepisu art. 6 ust. 1 lit. c RODO w celu prowadzenia przedmiotowego postępowania o udzielenie zamówienia publicznego oraz zawarcia umowy, a podstawą prawną ich przetwarzania jest obowiązek prawny stosowania sformalizowanych procedur udzielania zamówień publicznych spoczywających na administratorze danych, będącym zamawiającym.
4. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego. Konsekwencje niepodania określonych danych wynikają z przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych.
5. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o przepisy art. 18 oraz art. 74 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych.
6. Dane osobowe nie będą podlegać zautomatyzowanemu podejmowaniu decyzji i nie będą profilowane.
7. Dane osobowe będą przechowywane przez okres niezbędny do realizacji celów określonych powyżej, a po tym czasie przez okres oraz w zakresie wymaganym przez przepisy powszechnie obowiązującego prawa. Zgodnie z przepisami art. 78 ust. 1 i 4 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych protokół postępowania wraz z załącznikami będzie przechowywany przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, w sposób gwarantujący jego nienaruszalność, a jeżeli okres obowiązywania umowy w sprawie zamówienia publicznego przekroczy 4 lata, protokół postępowania wraz z załącznikami będzie przechowywany przez cały okres obowiązywania umowy w sprawie zamówienia publicznego.
8. Przysługuje Pani/Panu prawo żądania dostępu do treści danych osobowych, prawo żądania ich sprostowania oraz ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w przepisie art. 18 ust. 2 RODO.
9. Nie przysługuje Pani/Panu prawo do usunięcia danych osobowych, prawo do przenoszenia danych osobowych, a także prawo sprzeciwu wobec przetwarzania danych osobowych.
10. Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego, to jest Prezesa Urzędu Ochrony Danych Osobowych w przypadku uznania, że przetwarzanie danych osobowych narusza przepisy prawa.