

# GMINA POTOK GÓRNY

reprezentowana przez

Wójta Gminy

## SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego na zadanie:

**„Zakup sprzętu IT wraz z oprogramowaniem w ramach  
projektu Zwiększenie cyberbezpieczeństwa Gminy Potok  
Górny”**

**(Znak postępowania: IN.271.2.3.2026.AK)**

**ZATWIERDZAM**

**Wójt Gminy Potok Górny –Stanisław Dyjak**

**WÓJT GMINY**

*mgr inż. Stanisław Dyjak*

(podpis Kierownika Zamawiającego)

Potok Górny, maj 2026 r.

## 1. POSTANOWIENIA OGÓLNE

### 1.1. Nazwa oraz adres Zamawiającego.

Gmina Potok Górny zwana dalej „Zamawiającym”

Potok Górny 116, 23-423 Potok Górny,

NIP: 918-19-89-917, REGON: 950369155,

nr telefonu +48 (84) 685 25 00,

Adres poczty elektronicznej: [sekretariat@potokgorny.com.pl](mailto:sekretariat@potokgorny.com.pl)

Strona internetowa Zamawiającego [URL]: <https://ugpotokgorny.bip.lubelskie.pl>

**Adres strony internetowej prowadzonego postępowania:**

<https://ezamowienia.gov.pl/mp-client/search/list/ocds-148610-553a8d2b-9e87-43c9-a0ec-89afe9bd7726>

**Identyfikator (ID) postępowania na Platformie e-Zamówienia:** ocds-148610-553a8d2b-9e87-43c9-a0ec-89afe9bd7726

Postępowanie można wyszukać również ze strony głównej Platformy e-zamówienia przycisk „Przeglądaj postępowania/konkursy”.

- 1.2. Niniejsze postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym, w którym w odpowiedzi na ogłoszenie o zamówieniu oferty mogą składać wszyscy zainteresowani Wykonawcy, a następnie Zamawiający wybiera najkorzystniejszą ofertę bez przeprowadzenia negocjacji (art. 275 pkt 1 ustawy Pzp).

Zamawiający nie przewiduje możliwości wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji (art. 275 pkt 2 ustawy Pzp).

### 1.3. Słownik.

Użyte w niniejszej SWZ (oraz w załącznikach) terminy mają następujące znaczenie:

- 1) „**ustawa Pzp**” – ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (t. j. Dz. U. z 2024 r. poz. 1320 ze zm.),
- 2) „**SWZ**” – niniejsza Specyfikacja Warunków Zamówienia,
- 3) „**zamówienie**” – zamówienie publiczne będące przedmiotem niniejszego postępowania,
- 4) „**postępowanie**” – postępowanie o udzielenie zamówienia publicznego, którego dotyczy niniejsza SWZ,
- 5) „**Zamawiający**” – Gmina Potok Górny,
- 6) „**Wykonawca**” – należy przez to rozumieć osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która oferuje na rynku wykonanie robót budowlanych lub obiektu budowlanego, dostawę produktów lub świadczenie usług lub ubiega się o udzielenie zamówienia, złożyła ofertę lub zawarła umowę w sprawie zamówienia publicznego,
- 7) „**RODO**” - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1),
- 8) „**Platforma e-zamówienia**” – ogólnodostępne i nieodpłatne narzędzie informatyczne do obsługi postępowań o udzielenie zamówienia publicznego w tym przedmiotowego postępowania, w szczególności do elektronicznego składania ofert dostępne pod adresem: <https://ezamowienia.gov.pl>
- 9) „**kwalifikowany podpis elektroniczny**” – podpis wystawiony przez dostawcę kwalifikowanej usługi zaufania, będącego podmiotem świadczącym usługi certyfikacyjne - podpis elektroniczny, spełniający wymogi bezpieczeństwa określone w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2021 r., poz. 1797 z późn. zm.),
- 10) „**podpis zaufany**” – podpis elektroniczny, którego autentyczność i integralność są



zapewniane przy użyciu pieczęci elektronicznej ministra właściwego do spraw informatyzacji, zawierający dane identyfikujące osobę tj. imię (imiona), nazwisko, PESEL, ustalone na podstawie środka identyfikacji elektronicznej, identyfikator środka identyfikacji elektronicznej, przy użyciu, którego został złożony, czas jego złożenia,

- 11) „**podpis osobisty**” – zaawansowany podpis elektroniczny w rozumieniu art. 3 pkt 11 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE, weryfikowany za pomocą certyfikatu podpisu osobistego

- 1.4. Wykonawca powinien dokładnie zapoznać się z niniejszą SWZ i złożyć ofertę zgodnie z jej wymaganiami.

## 2. OZNACZENIE POSTĘPOWANIA

- 2.1. Postępowanie oznaczone jest znakiem: **IN.271.2.3.2026.AK**

- 2.2. Wykonawcy powinni we wszelkich kontaktach z Zamawiającym powoływać się na wyżej podane oznaczenie.

## 3. ŹRÓDŁA FINANSOWANIA

Zadanie realizowane jest w związku z realizacją projektu pn „**Zwiększenie cyberbezpieczeństwa Gminy Potok Górny**”, współfinansowanego ze środków Unii Europejskiej i budżetu państwa w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Priorytetu II Zaawansowane usługi cyfrowe, Działania 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.01-001/23/2520/ FERC.02.02-CS.01-001/23/2024.

## 4. OPIS PRZEDMIOTU ZAMÓWIENIA

- 4.1. Przedmiotem zamówienia jest zadanie pn. **Zakup sprzętu IT wraz z oprogramowaniem w ramach projektu Zwiększenie cyberbezpieczeństwa Gminy Potok Górny.**

- 4.2. Zakres zadania obejmuje w szczególności

Lp.	Nazwa	Ilość
<b>Część 1 Dostawa serwerów z oprogramowaniem</b>		
1.	Zakup serwera z oprogramowaniem typ I	1 szt.
2.	Zakup serwera z oprogramowaniem typ II	1 szt.
3.	Zakup i wdrożenie rozwiązania Network Access Control	1 kpl.
4.	Zakup oprogramowania do archiwizacji i kategoryzacji logów	1 kpl.
5.	Zakup oprogramowania do inwentaryzacji i ochrony przed wyciekiem DLP	1 kpl.
<b>Część 2 Dostawa przełączników sieciowych, serwera NAS oraz UPS - a</b>		
6.	Zakup serwer NAS	2 szt.
7.	Zakup przełącznika sieciowego zarządzalnego	3 szt.
8.	Zakup UPS	1 kpl.

- 1) W ramach realizacji zamówienia Wykonawca zobowiązuje się w szczególności do:
- dostawy sprzętu informatycznego oraz oprogramowania określonego w SOPZ,
  - instalacji, konfiguracji oraz uruchomienia dostarczonych urządzeń i systemów,
  - wdrożenia systemów informatycznych zgodnie z wymaganiami określonymi w SOPZ,



- d) integracji dostarczonych rozwiązań z istniejącą infrastrukturą informatyczną Zamawiającego, jeżeli jest to wymagane,
  - e) przeprowadzenia szkolenia administratorów Zamawiającego w zakresie obsługi dostarczonych systemów, jeżeli wymagane takie wynika z SOPZ,
  - f) przekazania dokumentacji technicznej oraz powdrożeniowej dotyczącej dostarczonych urządzeń i systemów.
- 2) Zamawiający wymaga, aby wszystkie oferowane urządzenia były fabrycznie nowe, nieużywane, nieregenerowane, kompletne, wyprodukowane nie wcześniej niż na 12 miesięcy przed jego dostarczeniem, dostarczone w opakowaniu oryginalnym (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Sprzęt musi być wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie oraz musi pochodzić z autoryzowanego kanału dystrybucyjnego. Nie dopuszcza się zastosowania urządzeń tzw. „refurbished”. Oferowane urządzenia nie mogą pochodzić z wystawy lub z ekspozycji, muszą być kompletne, wraz z niezbędnymi do działania przewodami, z odpowiednim oprogramowaniem, posiadać wymagane prawem atesty i certyfikaty.
- 3) Zamawiający wymaga, aby oferowane oprogramowanie było nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) musi być wolne od wad fizycznych i prawnych.
- 4) Wykonawca w ofercie musi uwzględnić wszystkie koszty związane z wykonaniem przedmiotu zamówienia, wraz z jego dostarczeniem i rozładunkiem w siedzibie Zamawiającego, montażem, konfiguracją oraz wdrożeniem.
- 4.3.** Szczegółowy zakres zamówienia określony jest w Specyfikacji Warunków Zamówienia oraz w załączonym do SWZ Szczegółowym Opisie Przedmiotu Zamówienia Załącznik nr 1 do SWZ oraz Projekt umowy stanowiący załącznik Nr 2 do SWZ.
- 4.4.** Wykonawcy mogą złożyć ofertę na jedną, kilka lub wszystkie części zamówienia. Zamawiający nie określa maksymalnej liczby części zamówienia, na które może zostać udzielone zamówienie jednemu Wykonawcy.
- 4.5. Nazwa/y i kod/y Wspólnego Słownika Zamówień: (CPV):**
- 30200000-1 - Urządzenia komputerowe
  - 48820000-2 - Serwery
  - 48823000-3 - Serwery plików
  - 32420000-3 - Urządzenia sieciowe
  - 30233000-1 - Urządzenia do przechowywania i odczytu danych
  - 31682520-1 - Awaryjne urządzenia wyłączeniowe
  - 31682530-4 - Awaryjne urządzenia energetyczne
  - 48517000-5 - Pakiety oprogramowania informatycznego
  - 48620000-0 - Systemy operacyjne
  - 48900000-7 - Różne pakiety oprogramowania i systemy
  - 72263000-6 - Usługi wdrażania oprogramowania
- 4.6. Rozwiązania równoważne.**
- 1) W przypadku zastosowania materiałów, urządzeń, wyrobów lub rozwiązań równoważnych, Wykonawca zobowiązany jest do ich wskazania w ofercie oraz do złożenia wraz z ofertą kart technicznych lub innych dokumentów potwierdzających, że oferowane rozwiązania równoważne spełniają wymagania Zamawiającego opisane w przedmiocie zamówienia.



- 2) Funkcjonalność przedmiotu zaoferowanego w ramach równoważności nie może być gorsza od funkcjonalności produktów wymienionych w opisie przedmiotu zamówienia, zaoferowana oferta w ramach równoważności musi spełniać warunki i zakres gwarancji na poziomie nie gorszym niż dla produktów wpisanych w opis przedmiotu zamówienia, wsparcie techniczne zaoferowanych produktów równoważnych nie może być gorsze niż dla produktów wymienionych w opisie przedmiotu zamówienia.
- 3) Jeżeli Wykonawca nie złoży ww. dokumentów lub złożone dokumenty będą niekompletne (nie potwierdzając w ten sposób równoważności oferty w zakresie opisanym w opisie przedmiotu zamówienia, Zamawiający będzie wzywał do ich złożenia/uzupełnienia).
- 4) W przypadku, gdy Wykonawca nie złoży w ofercie takich dokumentów, to rozumie się przez to, że do kalkulacji ceny oferty ujęto materiały i rozwiązania o parametrach nie niższych niż zaproponowane w opisie przedmiotu zamówienia.
- 5) Wszędzie tam, gdzie przedmiot zamówienia został opisany poprzez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę - opisowi takiemu towarzyszą wyrazy „lub równoważny”.
- 6) Jeżeli przedmiot zamówienia został opisany w sposób, o którym mowa w pkt 5, zamawiający wskazuje w opisie przedmiotu zamówienia kryteria stosowane w celu oceny równoważności.
- 7) Wszędzie tam, gdzie przedmiot zamówienia został opisany przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 Pzp, zamawiający dopuszcza rozwiązania równoważne opisywanym, a odniesieniu takiemu towarzyszą wyrazy „lub równoważne”.
- 8) W przypadku gdy opis przedmiotu zamówienia odnosi się do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 Pzp, a oferowane dostawy nie są zgodne z normami, ocenami technicznymi, specyfikacjami technicznymi i systemami referencji technicznych, do których opis przedmiotu zamówienia się odnosi, zamawiający nie odrzuci oferty pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107 Pzp, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.
- 9) W przypadku gdy opis przedmiotu zamówienia odnosi się do wymagań dotyczących wydajności lub funkcjonalności, o których mowa w art. 101 ust. 1 pkt 1 Pzp, zamawiający nie odrzuci oferty zgodnej z Polską Normą przenoszącą normę europejską, normami innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszącymi normy europejskie, z europejską oceną techniczną, ze wspólną specyfikacją techniczną, z normą międzynarodową lub z systemem referencji technicznych ustanowionym przez europejski organ normalizacyjny, jeżeli te normy, oceny techniczne, specyfikacje i systemy referencji technicznych dotyczą wymagań dotyczących wydajności lub funkcjonalności określonych przez zamawiającego, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107 Pzp, że dostawa spełnia wymagania dotyczące wydajności lub funkcjonalności określone przez zamawiającego.
- 10) Zgodnie z art. 101 ust. 5 Pzp wykonawca, który powołuje się na rozwiązania równoważne opisywanym w tych dokumentach, jest obowiązany udowodnić, poprzez dołączenie do oferty stosownych przedmiotowych środków dowodowych, o których mowa w art. 104-107 ustawy Pzp, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.

#### 4.7. Przedmiotowe środki dowodowe.



Zamawiający żąda innych niż wskazane w art. 104 i art. 105 przedmiotowych środków dowodowych na potwierdzenie, że oferowane dostawy, spełniają określone przez zamawiającego wymagania, cechy lub kryteria.

- 1) opis charakterystyki zaoferowanego sprzętu informatycznego i oprogramowania zawierający również nazwę producenta i model dla każdego z zaoferowanego sprzętu informatycznego oraz zaoferowanego oprogramowania. Opis, o którym mowa, powinien odnosić się do każdego z wymagań określonych w SOPZ w celu umożliwienia Zamawiającemu weryfikacji spełniania przez oferowany sprzęt informatyczny i oprogramowanie wymagań minimalnych określonych w SOPZ - Załącznik nr 8 do SWZ
  - 2) dla zaoferowanego modelu serwera Typ I, TypII, ( część 1 zamówienia): - raport z oprogramowania testującego w teście SPECrate2017\_fp\_base w standardzie organizacji Standard Performance Evaluation Corporation ([www.spec.org](http://www.spec.org)) potwierdzający minimalną liczbę punktów określoną w SOPZ dla procesora dedykowanego do pracy z zaoferowanym serwerem. Zamawiający dopuszcza złożenie dokumentu w języku angielskim;
  - 3) dla zaoferowanego modelu serwera NAS (część 2 zamówienia) - wydruk ze strony internetowej [www.cpubenchmark.net](http://www.cpubenchmark.net) potwierdzający wynik testów dla procesora zainstalowanego w oferowanym serwerze NAS, dopuszcza się wydruk w języku angielskim
- 4.7.1. Zamawiający akceptuje równoważne przedmiotowe środki dowodowe, jeśli potwierdzają, że oferowane dostawy spełniają określone przez Zamawiającego wymagania, cechy i kryteria.
- 4.7.2. Zamawiający informuje, że działając na podstawie art. 107 ust. 2 ustawy Pzp przewiduje, że w sytuacji, w której Wykonawca nie złożył przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe są niekompletne, Zamawiający jednokrotnie wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie.
- 4.7.3. Postanowień pkt 4.7.1 SWZ nie stosuje się pomimo złożenia przedmiotowego środka dowodowego, oferta podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania.
- 4.7.4. Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści przedmiotowych środków dowodowych.

## 5. TERMIN WYKONANIA ZAMÓWIENIA

- 5.1. Wykonawca jest zobowiązany wykonać zamówienie w terminie do **30 dni od dnia zawarcia umowy** (każda z części zamówienia)

## 6. INFORMACJE O WARUNKACH UDZIAŁU W POSTĘPOWANIU

- 6.1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki udziału w postępowaniu dotyczące:

**6.1.1. zdolności do występowania w obrocie gospodarczym;**

*Zamawiający nie określa warunku w ww. zakresie.*

**6.1.2. uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów;**

*Zamawiający nie określa warunku w ww. zakresie.*

### 6.1.3. uprawnień sytuacji ekonomicznej lub finansowej;

*Zamawiający nie określa warunku w ww. zakresie*

### 6.1.4. zdolności technicznej lub zawodowej w zakresie:

*Opis sposobu dokonywania oceny spełniania tego warunku:*

- 1) Określenie warunku w zakresie **części 1 zamówienia**: Zamawiający określa, że ww. warunek zostanie spełniony, jeśli Wykonawca wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie wykonał (a w przypadku świadczeń powtarzających się lub ciągłych nadal wykonuje), co najmniej jedno zamówienie obejmujące swoim zakresem dostawę sprzętu i oprogramowania informatycznego o wartości **nie mniejszej niż 150 000 zł brutto - w tym dostarczył co najmniej jeden serwer**. Przez zamówienie należy rozumieć: zamówienie rozpoczęte i zakończone w w/w okresie, zamówienie zakończone w w/w okresie, a rozpoczęte wcześniej niż w w/w okresie.
- 2) Określenie warunku w zakresie **części 2 zamówienia**: Zamawiający określa, że ww. warunek zostanie spełniony, jeśli Wykonawca wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie wykonał (a w przypadku świadczeń powtarzających się lub ciągłych nadal wykonuje), co najmniej jedno zamówienie obejmujące swoim zakresem dostawę sprzętu i oprogramowania informatycznego o wartości **nie mniejszej niż 50 000 zł brutto**. Przez zamówienie należy rozumieć: zamówienie rozpoczęte i zakończone w w/w okresie, zamówienie zakończone w w/w okresie, a rozpoczęte wcześniej niż w w/w okresie.

### 6.1.5. dodatkowe informacje dotyczące warunków udziału w postępowaniu:

- 1) W przypadku wspólnego ubiegania się o udzielenie zamówienia przez Wykonawców, Zamawiający uzna warunek dotyczący zdolności technicznej lub zawodowej, o którym mowa w 6.1.4. ppkt 1) za spełniony, gdy jeden z Wykonawców wykaże się realizacją jednego wymaganego przez Zamawiającego zamówienia. Zamawiający nie dopuszcza sumowania zdolności technicznej lub zawodowej, tzn. warunek, o którym mowa powyżej dla Części 1 zamówienia nie zostanie uznany za spełniony w sytuacji, gdy Wykonawcy wspólnie ubiegający się o zamówienie wykażą, że zrealizowali w sumie dostawy o łącznej wartości 150 000,00 zł brutto, lecz żaden z nich nie zrealizował samodzielnie jednej takiej dostawy o wymaganej przez Zamawiającego wartości.
- 2) W przypadku wspólnego ubiegania się o udzielenie zamówienia przez Wykonawców, Zamawiający uzna warunek dotyczący zdolności technicznej lub zawodowej, o którym mowa w 6.1.4. ppkt 2) za spełniony, gdy jeden z Wykonawców wykaże się realizacją jednego wymaganego przez Zamawiającego zamówienia. Zamawiający nie dopuszcza sumowania zdolności technicznej lub zawodowej, tzn. warunek, o którym mowa powyżej dla Części 2 zamówienia nie zostanie uznany za spełniony w sytuacji, gdy Wykonawcy wspólnie ubiegający się o zamówienie wykażą, że zrealizowali w sumie dostawy o łącznej wartości 50 000,00 zł brutto, lecz żaden z nich nie zrealizował samodzielnie jednej takiej dostawy o wymaganej przez Zamawiającego wartości.
- 3) Jeżeli Wykonawca powołuje się na doświadczenie w realizacji zamówień wykonywanych wspólnie z innymi wykonawcami, należy wykazać konkretny zakres, który został bezpośrednio zrealizowany przez Wykonawcę.



- 4) W przypadku, gdy Wykonawca polegający na zdolnościach lub sytuacji innych podmiotów w zakresie zdolności technicznej lub zawodowej, Zamawiający uzna warunek dotyczący zdolności technicznej lub zawodowej, o którym mowa w 6.1.4. ppkt 1) dla Części 1 zamówienia za spełniony, gdy podmiot udostępniający zdolność techniczną lub zawodową zrealizował samodzielnie jedno zamówienie wymagane przez Zamawiającego.
  - 5) W przypadku, gdy Wykonawca polegający na zdolnościach lub sytuacji innych podmiotów w zakresie zdolności technicznej lub zawodowej, Zamawiający uzna warunek dotyczący zdolności technicznej lub zawodowej, o którym mowa w 6.1.4. ppkt 2) dla Części 2 zamówienia za spełniony, gdy podmiot udostępniający zdolność techniczną lub zawodową zrealizował samodzielnie jedno zamówienie wymagane przez Zamawiającego.
  - 6) W przypadku, gdy Wykonawca składa ofertę na więcej niż jedną część zamówienia musi wykazać spełnianie warunków udziału w postępowaniu określonych dla każdej części odrębnie, przy czym Zamawiający dopuszcza możliwość wykazania spełniania tych warunków tym samym zamówieniem (jedną umową), o ile jego zakres i wartość odpowiadają wymaganiom określonym dla każdej części zamówienia.
  - 7) Wykonawca powinien w wykazie dostaw wyraźnie określić rodzaj zrealizowanych dostaw, aby można było ustalić, czy spełnia warunek udziału w postępowaniu.
  - 8) Wartości podane w dokumentach w walutach innych niż wskazane przez Zamawiającego będą przeliczane wg średniego kursu NBP na dzień publikacji ogłoszenia.
- 6.2. Zamawiający może, oceniając zdolność techniczną lub zawodową, 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 na każdym etapie postępowania (art. 116 ust. 2 ustawy Pzp).
- 6.3. W odniesieniu do warunków dotyczących, kwalifikacji zawodowych lub doświadczenia Wykonawcy wspólnie ubiegający się o udzielenie zamówienia wykazując warunek udziału w postępowaniu **mogą polegać na zdolnościach tych z wykonawców, którzy wykonają usługi, do realizacji których te zdolności są wymagane.**
- 6.4. Sposób wykazania warunków udziału w postępowaniu wskazano w rozdziale 8 SWZ.

## 7. PODSTAWY WYKLUCZENIA

- 7.1. Z postępowania o udzielenie zamówienia wyklucza się Wykonawcę, w stosunku, do którego zachodzi którakolwiek z okoliczności, o których mowa w art. 108 ustawy Pzp tj. jeżeli:
- 1) Wykonawca jest osobą fizyczną, którego prawomocnie skazano za przestępstwo:
    - a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
    - b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
    - c) o którym mowa w art. 228-230a, art. 250a Kodeksu karnego, w art. 46-48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2020 r. poz. 1133 oraz z 2021 r. poz. 2054) lub w art. 54 ust. 1-4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków

spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2021 r. poz. 523, 1292, 1559 i 2054),

- d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
- e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
- f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769 oraz z 2020 r. poz. 2023),
- g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,
- h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej

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

- 2) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;
  - 3) wobec Wykonawcy 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 Wykonawcy prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
  - 5) 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 wykazą, że przygotowali te oferty lub wnioski niezależnie od siebie;
  - 6) w przypadkach, o których mowa w art. 85 ust. 1, 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.
- 7.2. Zamawiający **nie przewiduje** podstaw wykluczenia wskazanych w art. 109 ust. 1 ustawy Pzp.
- 7.3. Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia

- 7.4. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2 i 5 ustawy Pzp, jeżeli udowodni Zamawiającemu, że spełnił łącznie następujące przesłanki
- 1) naprawił lub zobowiązał się do naprawienia szkody wyrządzonej przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem, w tym poprzez zadośćuczynienie pieniężne;
  - 2) wyczerpująco wyjaśnił fakty i okoliczności związane z przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem oraz spowodowanymi przez nie szkodami, aktywnie współpracując odpowiednio z właściwymi organami, w tym organami ścigania, lub zamawiającym;
  - 3) podjął konkretne środki techniczne, organizacyjne i kadrowe, odpowiednie dla zapobiegania dalszym przestępstwom, wykroczeniom lub nieprawidłowemu postępowaniu, w szczególności:
    - a) zerwał wszelkie powiązania z osobami lub podmiotami odpowiedzialnymi za nieprawidłowe postępowanie wykonawcy,
    - b) zreorganizował personel,
    - c) wdrożył system sprawozdawczości i kontroli,
    - d) utworzył struktury audytu wewnętrznego do monitorowania przestrzegania przepisów, wewnętrznych regulacji lub standardów,
    - e) wprowadził wewnętrzne regulacje dotyczące odpowiedzialności i odszkodowań za nieprzestrzeganie przepisów, wewnętrznych regulacji lub standardów.
- 7.5. Zamawiający ocenia, czy podjęte przez wykonawcę czynności wskazane w pkt 7.4 SWZ są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu wykonawcy. Jeżeli podjęte przez wykonawcę czynności wskazane w pkt 7.4 SWZ nie są wystarczające do wykazania jego rzetelności, zamawiający wyklucza wykonawcę
- 7.6. Wykonawca podlega wykluczeniu także w oparciu o podstawy wykluczenia wskazane art. 7 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t. j. Dz. U. 2022 r., poz. 835 z późn. zm.).
- 7.7. Zamawiający informuje, że wykluczeniu z postępowania na podstawie pkt 7.6 SWZ podlegają:
- 1) wykonawcy wymienieni w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006, str. 1, z późn. zm.3) i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014, str. 6, z późn. zm.4) albo wpisani na listę o której mowa w art. 2 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, na podstawie decyzji w sprawie wpisu na ww. listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 powołanej ustawy;
  - 2) wykonawcy, których beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006, str. 1, z późn. zm.3) i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań





podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014, str. 6, z późn. zm.4)) albo wpisani na listę o której mowa w art. 2 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, lub będący takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile zostali wpisani na ww. listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego .;

- 3) wykonawcy, których jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106) jest podmiot wymieniony w wykazach określonych w rozporządzeniu Rady (WE) nr 765/2006 z dnia 18 maja 2006 r. dotyczącego środków ograniczających w związku z sytuacją na Białorusi i udziałem Białorusi w agresji Rosji wobec Ukrainy (Dz. Urz. UE L 134 z 20.05.2006, str. 1, z późn. zm.3) i rozporządzeniu Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających w odniesieniu do działań podważających integralność terytorialną, suwerenność i niezależność Ukrainy lub im zagrażających (Dz. Urz. UE L 78 z 17.03.2014, str. 6, z późn. zm.4)) albo wpisani na listę o której mowa w art. 2 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na ww. listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.
- 7.8. Wykluczenie, o którym mowa w pkt 7.6 SWZ następuje na okres trwania ww. okoliczności.
- 7.9. W przypadku Wykonawcy wykluczonego na podstawie przesłanek wskazanych w pkt 7.7 SWZ, Zamawiający odrzuca ofertę takiego Wykonawcy.
- 7.10. Osoba lub podmiot podlegające wykluczeniu, które w okresie tego wykluczenia ubiegają się o udzielenie zamówienia publicznego lub biorą udział w postępowaniu o udzielenie zamówienia publicznego, podlegają karze pieniężnej. Karę pieniężną, nakłada Prezes Urzędu Zamówień Publicznych, w drodze decyzji, w wysokości do 20 000 000 zł.
- 7.11. Sposób wykazania braku podstaw wykluczenia wskazano w rozdziale 8 SWZ.

## 8. INFORMACJA O OŚWIADCZENIU WSTĘPNYM I PODMIOTOWYCH ŚRODKACH DOWODOWYCH

- 8.1. Wykonawca zobowiązany jest złożyć wraz z ofertą oświadczenia stanowiące wstępne potwierdzenie, że Wykonawca na dzień składania ofert:
- a) nie podlega wykluczeniu,
  - b) spełnia warunki udziału w postępowaniu.
- 8.1.1. Oświadczenia należy złożyć wg wymogów załącznika nr 4 do SWZ.
- 8.1.2. Jeżeli Wykonawca nie złożył oświadczeń, o których mowa w pkt 8.1 SWZ lub są one niekompletne lub zawierają błędy, Zamawiający wezwie Wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w wyznaczonym terminie, chyba że oferta Wykonawcy podlega odrzuceniu bez względu na ich złożenie, uzupełnienie lub poprawienie lub zachodzą przesłanki unieważnienia postępowania.



- 8.1.3. Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych oświadczeń, o których mowa w pkt 8.1 SWZ.
- 8.1.4. Jeżeli złożone przez Wykonawcę oświadczenia, o których mowa w pkt 8.1 SWZ budzą wątpliwości Zamawiającego, może on zwrócić się bezpośrednio do podmiotu, który jest w posiadaniu informacji lub dokumentów istotnych w tym zakresie dla oceny spełniania przez Wykonawcę warunków udziału w postępowaniu lub braku podstaw wykluczenia, o przedstawienie takich informacji lub dokumentów.
- 8.1.5. Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści oświadczenia, o których mowa w pkt 8.1 SWZ.
- 8.2. W przypadku, o którym mowa w punkcie 6.3 SWZ Wykonawcy wspólnie ubiegający się o udzielenie zamówienia **dołączają do oferty** oświadczenie, z którego wynika, które dostawy lub usługi wykonają poszczególni wykonawcy. W przypadku gdy ofertę składa spółka cywilna, a pełen zakres prac wykonają wspólnicy wspólnie w ramach umowy spółki oświadczenie powinno potwierdzać ten fakt. **Oświadczenie należy złożyć wg wymogów załącznika nr 6 do SWZ.**
- 8.3. Zamawiający **wezwe Wykonawcę**, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie (nie krótszym niż 5 dni od dnia wezwania) następujących podmiotowych środków dowodowych (aktualnych na dzień złożenia):
- 8.3.1. **W celu potwierdzenia spełniania warunków udziału w postępowaniu** (w zakresie odpowiednio dla Części 1 i 2):
- a) wykaz dostaw wykonanych, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy lub usługi zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów - oświadczenie wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy – zgodnie z wzorem stanowiącym **Załącznik nr 7 do SWZ – w odniesieniu do warunku określonego w pkt 6.1.4 pkt. 1) SWZ**,
- 8.3.2. **W celu potwierdzenia braku podstaw do wykluczenia z udziału w postępowaniu:**
- Zamawiający **nie wymaga** złożenia przez Wykonawcę podmiotowych środków dowodowych w tym zakresie.
- 8.4. Jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, Zamawiający może na każdym etapie postępowania wezwać Wykonawców do złożenia wszystkich lub niektórych podmiotowych środków dowodowych wskazanych w pkt. 8.3.1 SWZ.
- 8.5. Wykonawca składa podmiotowe środki dowodowe na wezwanie Zamawiającego. Dokumenty te powinny być aktualne na dzień ich złożenia.
- 8.6. Jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio podmiotowe środki dowodowe nie są już aktualne, Zamawiający może w każdym czasie wezwać Wykonawcę lub Wykonawców do złożenia wszystkich lub niektórych podmiotowych środków dowodowych, aktualnych na dzień ich złożenia.

- 8.7. Zamawiający nie będzie wzywał do złożenia podmiotowych środków dowodowych, jeżeli może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile wykonawca wskazał w oświadczeniu, o którym mowa w pkt 8.1 SWZ dane umożliwiające dostęp do tych środków.
- 8.8. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które Zamawiający posiada, jeżeli Wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.
- 8.9. Jeżeli Wykonawca nie złożył podmiotowych środków dowodowych lub są one niekompletne lub zawierają błędy, Zamawiający wezwie Wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w wyznaczonym terminie, chyba że oferta Wykonawcy podlega odrzuceniu bez względu na ich złożenie, uzupełnienie lub poprawienie lub zachodzą przesłanki unieważnienia postępowania.
- 8.10. Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych podmiotowych środków dowodowych.
- 8.11. Jeżeli złożone przez Wykonawcę podmiotowe środki dowodowe budzą wątpliwości Zamawiającego, może on zwrócić się bezpośrednio do podmiotu, który jest w posiadaniu informacji lub dokumentów istotnych w tym zakresie dla oceny spełniania przez wykonawcę warunków udziału w postępowaniu, kryteriów selekcji lub braku podstaw wykluczenia, o przedstawienie takich informacji lub dokumentów.
- 8.12. Oświadczenia o których mowa w rozdziale 8.1 SWZ składa się, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.
- 8.13. Podmiotowe środki dowodowe sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, z zastrzeżeniem formatów, o których mowa w art. 66 ust. 1 ustawy, z uwzględnieniem rodzaju przekazywanych danych.
- 8.14. Podmiotowe środki dowodowe przekazuje się wg zasad określonych w rozporządzeniu Prezesa Rady Ministrów w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz.U.2020 poz. 2452).
- 8.15. W przypadku przekazywania 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.
- 8.16. Oświadczenia wskazane w rozdziale 8.1 SWZ i podmiotowe środki dowodowe przekazuje się środkiem komunikacji elektronicznej wskazanym w rozdziale 11 SWZ.
- 8.17. W przypadku, gdy oświadczenia o których mowa w rozdziale 8.1 SWZ lub podmiotowe środki dowodowe zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233 ze zm.), Wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku.
- 8.18. Podmiotowe środki dowodowe sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski.
- 8.19. Dokumenty elektroniczne muszą spełniać łącznie następujące wymagania:



- 1) są utrwalone w sposób umożliwiający ich wielokrotne odczytanie, zapisanie i powielenie, a także przekazanie przy użyciu środków komunikacji elektronicznej lub na informatycznym nośniku danych;
- 2) umożliwiają prezentację treści w postaci elektronicznej, w szczególności przez wyświetlenie tej treści na monitorze ekranowym;
- 3) umożliwiają prezentację treści w postaci papierowej, w szczególności za pomocą wydruku;
- 4) zawierają dane w układzie niepozostawiającym wątpliwości co do treści i kontekstu zapisanych informacji.

## 9. INFORMACJA DLA WYKONAWCÓW POLEGAJĄCYCH NA ZASOBACH INNYCH PODMIOTÓW, NA ZASADACH OKREŚLONYCH W ART. 118 USTAWY PZP ORAZ ZAMIERZAJĄCYCH POWIERZYĆ WYKONANIE CZĘŚCI ZAMÓWIENIA PODWYKONAWCOM

- 9.1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu lub kryteriów selekcji, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.
- 9.2. Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.
- 9.3. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, **jeśli podmioty te wykonają dostawy, do realizacji których te zdolności są wymagane.**
- 9.4. 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.
- 9.5. Zobowiązanie podmiotu udostępniającego zasoby lub inny środek dowodowy, o którym mowa w pkt 9.4 SWZ potwierdza, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
  - 1) zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
  - 2) sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
  - 3) czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą.
- 9.6. Zamawiający oceni, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu, a także zbada, czy nie zachodzą, wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem wykonawcy.

- 9.7. 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 zażąda, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.
- 9.8. Wykonawca, w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby, przedstawia, wraz z oświadczeniami, o którym mowa w pkt 8.1 SWZ także oświadczenia podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim Wykonawca powołuje się na jego zasoby **wg wymogów Załącznika nr 5 do SWZ**.
- 9.9. Zamawiający **nie żąda** wskazania przez Wykonawcę, w ofercie, części zamówienia, których wykonanie zamierza powierzyć podwykonawcom, którzy nie są podmiotami udostępniającymi zasoby, oraz podania nazw ewentualnych podwykonawców.
- 9.10. Wykonawca będzie zobowiązany do zawiadamiania Zamawiającego o wszelkich zmianach w odniesieniu do informacji, o których mowa w pkt 9.1 SWZ, w trakcie realizacji zamówienia, a także przekazać wymagane informacje na temat nowych podwykonawców, którym w późniejszym okresie zamierza powierzyć realizację robót budowlanych lub usług.

## 10. INFORMACJA DLA WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA (W TYM SPÓŁKI CYWILNE)

- 10.1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku, Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
- 10.2. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia:
- 1) oświadczenia o których mowa w pkt. 8.1 SWZ **składa z ofertą każdy z Wykonawców wspólnie ubiegających się o zamówienie**. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu
  - 2) w przypadku, o którym mowa w rozdziale 6.3 SWZ Wykonawcy wspólnie ubiegający się o udzielenie zamówienia **dołączają do oferty** oświadczenie, z którego wynika, które dostawy wykonają poszczególni Wykonawcy. W przypadku gdy ofertę składa spółka cywilna, a pełen zakres prac wykonają wspólnicy wspólnie w ramach umowy spółki oświadczenie powinno potwierdzać ten fakt.
  - 3) zobowiązani są oni na wezwanie Zamawiającego, złożyć podmiotowe środki dowodowe, o których mowa w pkt. 8.3 SWZ, przy czym podmiotowe środki dowodowe, o których mowa w pkt. 8.3.1 SWZ składa odpowiednio Wykonawca/Wykonawcy, który/którzy wykazuje/-ą spełnienie warunku.
- 10.3. Jeżeli została wybrana oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Zamawiający może żądać przed zawarciem umowy w sprawie zamówienia publicznego kopii umowy regulującej współpracę tych Wykonawców.

## 11. 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

- 11.1. W postępowaniu o udzielenie zamówienia publicznego komunikacja między Zamawiającym a wykonawcami odbywa się przy użyciu Platformy e-Zamówienia, która jest dostępna pod adresem <https://ezamowienia.gov.pl>.
- 11.2. Korzystanie z Platformy e-Zamówienia jest bezpłatne.
- 11.3. Zamawiający wyznacza następujące osoby do kontaktu z wykonawcami: **Pan Andrzej Kuś**, tel. 84 685 25 18, e-mail: [sekretariat@potokgorny.com.pl](mailto:sekretariat@potokgorny.com.pl).
- 11.4. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego musi posiadać konto podmiotu „Wykonawca” na Platformie e-Zamówienia. Szczegółowe informacje na temat zakładania kont podmiotów oraz zasady i warunki korzystania z Platformy e-Zamówienia określa Regulamin Platformy e-Zamówienia, dostępny na stronie internetowej <https://ezamowienia.gov.pl/pl/regulamin/#regulamin-serwisu> oraz informacje zamieszczone w zakładce „Centrum Pomocy”.
- 11.5. Przeglądanie i pobieranie publicznej treści dokumentacji postępowania nie wymaga posiadania konta na Platformie e-Zamówienia ani logowania do Platformy e-Zamówienia.
- 11.6. Sposób sporządzenia dokumentów elektronicznych lub dokumentów elektronicznych będących kopią elektroniczną treści zapisanej w postaci papierowej (cyfrowe odwzorowania) musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie.
- 11.7. Dokumenty elektroniczne, o których mowa w § 2 ust. 1 rozporządzenia, o którym mowa w pkt. 11.6 SWZ, sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach 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, z uwzględnieniem rodzaju przekazywanych danych i przekazuje się jako załączniki. W przypadku formatów, o których mowa w art. 66 ust. 1 ustawy Pzp, ww. regulacje nie będą miały bezpośredniego zastosowania.
- 11.8. Informacje, oświadczenia lub dokumenty, inne niż wymienione w § 2 ust. 1 rozporządzenia, o którym mowa w pkt 11.6 SWZ, przekazywane w postępowaniu sporządza się w postaci elektronicznej:
  - a) w formatach danych określonych w przepisach rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności z uwzględnieniem rodzaju przekazywanych danych (i przekazuje się jako załącznik),
  - lub
  - b) jako tekst wpisany bezpośrednio do wiadomości przekazywanej przy użyciu środków komunikacji elektronicznej (np. w treści wiadomości e-mail lub w treści „Formularza do komunikacji”).
- 11.9. Jeżeli dokumenty elektroniczne, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233 ze zm.) wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem w nazwie pliku „Dokument stanowiący tajemnicę przedsiębiorstwa”.
- 11.10. Komunikacja w postępowaniu, z wyłączeniem składania ofert (sposób składania ofert opisano w rozdziale 13 SWZ) odbywa się drogą elektroniczną za pośrednictwem formularzy do komunikacji dostępnych w zakładce „Formularze” („Formularze do komunikacji”). Za



pośrednictwem „Formularzy do komunikacji” odbywa się w szczególności przekazywanie wezwań i zawiadomień, zadawanie pytań i udzielanie odpowiedzi. Formularze do komunikacji umożliwiają również dołączenie załącznika do przesyłanej wiadomości (przycisk „dodaj załącznik”).

- 11.11.** Możliwość korzystania w postępowaniu z „Formularzy do komunikacji” w pełnym zakresie wymaga posiadania konta „Wykonawcy” na Platformie e-Zamówienia oraz zalogowania się na Platformie e-Zamówienia. Do korzystania z „Formularzy do komunikacji” służących do zadawania pytań dotyczących treści dokumentów zamówienia wystarczające jest posiadanie tzw. konta uproszczonego na Platformie e-Zamówienia.
- 11.12.** Wszystkie wysłane i odebrane w postępowaniu przez wykonawcę wiadomości widoczne są po zalogowaniu w podglądzie postępowania w zakładce „Komunikacja”.
- 11.13.** Maksymalny rozmiar plików przesyłanych za pośrednictwem „Formularzy do komunikacji” wynosi 150 MB (wielkość ta dotyczy plików przesyłanych jako załączniki do jednego formularza).
- 11.14.** Minimalne wymagania techniczne dotyczące sprzętu używanego w celu korzystania z usług Platformy e-Zamówienia oraz informacje dotyczące specyfikacji połączenia określa § 12 Regulamin Platformy e-Zamówienia, a mianowicie:
- 11.14.1.** W celu prawidłowego korzystania z usług Platformy e-Zamówienia wymagany jest:
- a) Komputer PC:
    - parametry minimum: Intel Core2 Duo, 2 GB RAM, HD,
    - zainstalowany jeden z poniższych systemów operacyjnych: MS Windows 7 lub nowszy, OSX/Mac OS 10.10, Ubuntu 14.04,
    - zainstalowana jedna z poniższych przeglądarek: Chrome 66.0 lub nowsza, Firefox 59.0 lub nowszy, Safari 11.1 lub nowsza, Edge 14.0 i nowsze,albo
  - b) Tablet/Telefon:
    - parametry minimum: 4 rdzenie procesora, 2GB RAM, Android 6.0 Marshmallow, iOS 10.3,
    - przeglądarka Chrome 61 lub nowa
- 11.14.2.** Dla skorzystania z pełnej funkcjonalności może być konieczne włączenie w przeglądarce obsługi protokołu bezpiecznej transmisji danych SSL, obsługi Java Script, oraz cookies;
- 11.14.3.** Specyfikacja połączenia, formatu przesyłanych danych oraz kodowania i oznaczania czasu odbioru danych:
- a) specyfikacja połączenia – formularze udostępnione są za pomocą protokołu TLS 1.2,
  - b) format danych oraz kodowanie: formularze dostępne są w formacie HTML z kodowaniem UTF-8,
  - c) oznaczenia czasu odbioru danych: wszelkie operacje opierają się o czas serwera i dane zapisywane są z dokładnością co do sekundy.
- 11.15.** W przypadku problemów technicznych i awarii związanych z funkcjonowaniem Platformy e-Zamówienia użytkownicy mogą skorzystać ze wsparcia technicznego dostępnego pod numerem telefonu (32) 77 88 999 lub drogą elektroniczną poprzez formularz udostępniony na stronie internetowej <https://ezamowienia.gov.pl> w zakładce „Zgłoś problem”.
- 11.16.** W szczególnie uzasadnionych przypadkach uniemożliwiających komunikację Wykonawcy i Zamawiającego za pośrednictwem Platformy e-Zamówienia, Zamawiający dopuszcza komunikację za pomocą poczty elektronicznej na adres e-mai:



sekretariat@potokgorny.com.pl (nie dotyczy składania ofert w postępowaniu).

- 11.17. UWAGA: Zamawiający nie ponosi odpowiedzialności za błędy w transmisji danych, w tym błędy spowodowane awariami systemów teleinformatycznych, systemów zasilania lub też okolicznościami zależnymi od operatora zapewniającego transmisję danych.**

## **12. WYMAGANIA DOTYCZĄCE WADIUM**

Zamawiający nie wymaga wniesienia wadium.

## **13. OPIS SPOSOBU PRZYGOTOWANIA OFERTY**

- 13.1.** Każdy Wykonawca może złożyć ofertę na każdą z części zamówienia. Złożenie więcej niż jednej oferty na daną część spowoduje odrzucenie wszystkich ofert złożonych przez Wykonawcę.
- 13.2.** Zamawiający **dopuszcza** możliwość składania ofert częściowych wg podziału określonego w Rozdziale 4 SWZ
- 13.3.** Oferta musi być sporządzona w języku polskim.
- 13.4.** Ofertę składa się, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym w formatach danych określonych w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2021 r. poz. 2070 z późn. zm.) z zastrzeżeniem formatów, o których mowa w art. 66 ust. 1 ustawy Pzp, z uwzględnieniem rodzaju przekazywanych danych.
- 13.5.** Każdy dokument składający się na ofertę lub złożony wraz z ofertą sporządzony w języku innym niż polski musi być złożony wraz z tłumaczeniem na język polski.
- 13.6.** Treść oferty musi być zgodna z treścią SWZ.
- 13.7.** Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.
- 13.8.** Wykonawca składa ofertę poprzez Platformę e-Zamówienia za pośrednictwem zakładki „Oferty/wnioski”, widocznej w podglądzie postępowania po zalogowaniu się na konto Wykonawcy. Po wybraniu przycisku „Złóż ofertę” system prezentuje okno składania oferty umożliwiające przekazanie dokumentów elektronicznych, w którym znajdują się dwa pola drag&drop („przeciągnij” i „upuść”) służące do dodawania plików.
- 13.9.** Wykonawca dodaje wybrany z dysku i uprzednio podpisany „Formularz oferty – Załącznik Nr 3 do SWZ” w pierwszym polu („Wypełniony formularz oferty”). W kolejnym polu („Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”) Wykonawca dodaje pozostałe pliki stanowiące ofertę lub składane wraz z ofertą.

### **UWAGA:**

W związku z tym, że Zamawiający udostępnia Wykonawcom własny "Formularz oferty" (tj. nie za pośrednictwem interaktywnego "Formularza ofertowego", który umożliwia Platforma e-zamówienia), podczas czynności składania oferty może pojawić się komunikat o następującej treści "Czy chcesz kontynuować? Postępowanie nie posiada opublikowanego formularza do tego etapu postępowania. Plik [w tym miejscu pojawia się nazwa pliku] nie jest poprawnym formularzem interaktywnym wygenerowanym na Platformie." W takim przypadku należy wybrać opcję "Tak, chcę kontynuować".

- 13.10.** Formularz ofertowy podpisuje się kwalifikowanym podpisem elektronicznym, podpisem

zaufanym lub podpisem osobistym. Rekomendowanym wariantem podpisu jest typ wewnętrzny. Podpis formularza ofertowego wariantem podpisu w typie zewnętrznym również jest możliwy, tylko w tym przypadku, powstały oddzielny plik podpisu dla tego formularza należy załączyć w polu „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”.

- 13.11. Pozostałe dokumenty wchodzące w skład oferty lub składane wraz z ofertą, które są zgodne z ustawą Pzp lub 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 opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, mogą być zgodnie z wyborem wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia/podmiotu udostępniającego zasoby opatrzone podpisem typu zewnętrznego lub wewnętrznego. W zależności od rodzaju podpisu i jego typu (zewnętrzny, wewnętrzny) w polu „Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę” dodaje się uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny).
- 13.12. W przypadku przekazywania 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.
- 13.13. System sprawdza, czy złożone pliki są podpisane i automatycznie je szyfruje, jednocześnie informując o tym Wykonawcę. Potwierdzenie czasu przekazania i odbioru oferty znajduje się w Elektronicznym Potwierdzeniu Przesłania (EPP) i Elektronicznym Potwierdzeniu Odebrania (EPO). EPP i EPO dostępne są dla zalogowanego Wykonawcy w zakładce „Oferty/Wnioski”.
- 13.14. Maksymalny łączny rozmiar plików stanowiących ofertę lub składanych wraz z ofertą to 250 MB.
- 13.15. Na potrzeby oceny ofert oferta musi zawierać :
- 1) **Formularz ofertowy** –do wykorzystania wzór (druk), stanowiący Załącznik nr 3 do SWZ (przy czym Wykonawca może sporządzić ofertę wg innego wzorca, powinna ona wówczas obejmować dane wymagane dla oferty w SWZ i załącznikach);  
**Uwaga: Wykonawca ma obowiązek wskazać w Formularzu ofertowym: producenta, model, nazwę oferowanego urządzenia/oprogramowania. W przypadku, gdy Wykonawca nie wskaże producenta lub modelu lub nazwy oferowanego urządzenia/oprogramowania Zamawiający odrzuci ofertę na podstawie art. 226 ust. 1 pkt 5) ustawy Pzp, z zastrzeżeniem art. 223 ustawy Pzp.**
  - 2) **Potwierdzenie oferowanych parametrów (załącznik nr 9 do SWZ)** Załącznik stanowi oświadczenie Wykonawcy, że oferowany sprzęt spełnia wszystkie wymagane parametry techniczne określone przez Zamawiającego w OPZ.
  - 3) **Przedmiotowe środki dowodowe, o których mowa w pkt. 4.7 SWZ.**
  - 4) **Oświadczenie wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia składane na podstawie art. 125 ust. 1 ustawy Pzp, o którym mowa w pkt. 8.1 SWZ;**
  - 5) **Oświadczenie, o których mowa w pkt. 8.2 SWZ (jeżeli dotyczy);**
  - 6) **Zobowiązanie lub inne dokumenty, o których mowa w pkt. 9.4 SWZ (jeżeli dotyczy).**



- 7) **Oświadczenie podmiotu udostępniającego zasoby składane na podstawie art. 125 ust. 1 ustawy Pzp, o którym mowa w pkt. 9.8 SWZ (jeżeli dotyczy),**
- 8) **Potwierdzenie umocowania do działania w imieniu Wykonawcy lub podmiotu udostępniającego zasoby:**
- a) Zamawiający w celu potwierdzenia, że osoba działająca w imieniu Wykonawcy lub podmiotu udostępniającego zasoby jest umocowana do jego reprezentowania, żąda złożenia wraz z ofertą odpisu lub informacji z Krajowego Rejestru Sądowego, Centralnej Ewidencji I Informacji o Działalności Gospodarczej lub innego właściwego rejestru;
  - b) Wykonawca lub podmiot udostępniający zasoby nie jest zobowiązany do złożenia dokumentów, o których mowa w lit a), jeżeli Zamawiający może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, o ile Wykonawca wskazał dane umożliwiające dostęp do tych dokumentów.
  - c) jeżeli w imieniu Wykonawcy lub podmiotu udostępniającego zasoby działa osoba, której umocowanie do jego reprezentowania nie wynika z dokumentów, o których mowa w lit a), Zamawiający żąda od Wykonawcy lub podmiotu udostępniającego zasoby złożenia wraz z ofertą pełnomocnictwa lub innego dokumentu potwierdzającego umocowanie do reprezentowania Wykonawcy.
- 9) **Pełnomocnictwo do reprezentowania wykonawców wspólnie ubiegających się o udzielenie zamówienia w postępowaniu o udzielenie zamówienia albo do reprezentowania ich w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego (jeżeli dotyczy).**
- 13.16. Pełnomocnictwo o którym mowa w rozdziale 13.14 pkt 8) lit c) i pkt 9) SWZ składa się, pod rygorem nieważności w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym lub w formie elektronicznej kopii poświadczonej za zgodność notarialnie -w formatach danych określonych w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023r. poz. 57 ze zm.), z zastrzeżeniem formatów, o których mowa w art. 66 ust. 1 ustawy, z uwzględnieniem rodzaju przekazywanych danych.
- 13.17. Wszelkie informacje stanowiące **tajemnicę przedsiębiorstwa** w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233 ze zm.), które Wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać **złożone w osobnym pliku** wraz z jednoczesnym zaznaczeniem polecenia „*Dokument stanowiący tajemnicę przedsiębiorstwa*”, a następnie wraz z plikami stanowiącymi jawną część skompresowane do jednego pliku (ZIP). Wykonawca zobowiązany jest, wraz z przekazaniem tych informacji, wykazać spełnienie przesłanek określonych w art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Zaleca się, aby uzasadnienie zastrzeżenia informacji jako tajemnicy przedsiębiorstwa było sformułowane w sposób umożliwiający jego udostępnienie. Zastrzeżenie przez Wykonawcę tajemnicy przedsiębiorstwa bez uzasadnienia, będzie traktowane przez Zamawiającego jako bezskuteczne ze względu na zaniechanie przez Wykonawcę podjęcia niezbędnych działań w celu zachowania poufności objętych klauzulą informacji zgodnie z postanowieniami art. 18 ust. 3 ustawy.
- 13.18. Wykonawca nie może zastrzec informacji, o których mowa w art. 222 ust. 5 ustawy Pzp.
- 13.19. Oświadczenia i dokumenty, o których mowa w pkt. 13.16 SWZ sporządza się pod rygorem nieważności w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.



## 14. SKŁADANIE I OTWARCIE OFERT

- 14.1. Wykonawca składa ofertę za pomocą Platformy e-Zamówienia dostępnej pod adresem: <https://ezamowienia.gov.pl>.
- 14.2. Termin składania ofert: **18 maja 2026 r., godzina 10:00.**
- 14.3. Termin otwarcia ofert: **18 maja 2026 r., godzina 10:30.**
- 14.4. Oferta może być złożona tylko do upływu terminu składania ofert.
- 14.5. Wykonawca może przed upływem terminu składania ofert wycofać ofertę. Wykonawca wycofuje ofertę w zakładce „Oferty/wnioski” używając przycisku „Wycofaj ofertę”.
- 14.6. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
- 14.7. Otwarcie ofert następuje poprzez użycie mechanizmu do odszyfrowania ofert dostępnego po zalogowaniu w zakładce „Oferty/wnioski”.
- 14.8. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o:
  - 1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
  - 2) cenach lub kosztach zawartych w ofertach.
- 14.9. Zamawiający odrzuca ofertę, jeżeli została złożona po terminie składania ofert, o którym mowa w pkt. 14.2 SWZ.
- 14.10. W przypadku wystąpienia awarii systemu teleinformatycznego, która spowoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.

## 15. TERMIN ZWIĄZANIA OFERTĄ

- 15.1. Wykonawca jest związany ofertą do dnia **16-06-2026r.**
- 15.2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą, o którym mowa w pkt 15.1 SWZ, Zamawiający przed upływem terminu związania ofertą, zwróci się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.
- 15.3. Przedłużenie terminu związania ofertą, o którym mowa w pkt. 15.2 SWZ, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.
- 15.4. W przypadku, gdy Zamawiający żąda wniesienia wadium, przedłużenie terminu związania ofertą, o którym mowa pkt. 15.2 SWZ, następuje wraz z przedłużeniem okresu ważności wadium albo jeżeli nie jest to możliwe, z wniesieniem nowego wadium na przedłużony okres związania ofertą.

## 16. OPIS SPOSOBU OBLICZENIA CENY OFERTY

- 16.1. Obowiązującą formą wynagrodzenia za wykonanie przez Wykonawcę przedmiotu zamówienia będzie **wynagrodzenie ryczałtowe** wskazane w **Formularzu ofertowym – Załącznik Nr 3 do SWZ**. Cena ryczałtowa obejmuje wszystkie koszty i składniki związane z wykonaniem zamówienia w zakresie wynikającym z opisu przedmiotu zamówienia.

- 16.2. Cena winna uwzględniać wymagania wskazane w dokumentacji opisującej przedmiot zamówienia, SWZ i projekcie umowy.
- 16.3. Wykonawca powinien wyliczyć cenę oferty brutto, tj. wraz z należnym podatkiem VAT w wysokości przewidzianej ustawowo.
- 16.4. Wszelkie rozliczenia dotyczące realizacji przedmiotu zamówienia opisanego w niniejszej specyfikacji dokonywane będą w złotych polskich.
- 16.5. Jeżeli została złożona oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (t.j. Dz.U. z 2022 r. poz. 931 z późn. zm.), dla celów zastosowania kryterium ceny lub kosztu zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć.
- 16.6. W ofercie, o której mowa w pkt. 16.5 SWZ Wykonawca ma obowiązek:
- a) poinformowania Zamawiającego, że wybór jego oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego;
  - b) wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;
  - c) wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym Zamawiającego, bez kwoty podatku;
  - d) wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.
- 16.7. W Formularzu oferty Wykonawca podaje cenę, z dokładnością do dwóch miejsc po przecinku w rozumieniu art. 3 ust. 1 pkt 1 i ust. 2 ustawy z dnia 9 maja 2014r. o informowaniu o cenach towarów i usług oraz ustawy z dnia 7 lipca 1994 r. o denominacji złotego, za którą podejmuje się zrealizować przedmiot zamówienia.
- 16.8. Wynagrodzenie będzie płatne zgodnie z Projektem umowy **Załącznik Nr 2 do SWZ.**

## 17. OPIS KRYTERIÓW OCENY OFERT, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

- 17.1. Na podstawie art. 246 ust. 2 Ustawy Zamawiający może zastosować kryterium ceny jako jedyne kryterium oceny z uwagi na fakt, iż standardy jakościowe –parametry techniczne odnoszące się do wszystkich istotnych cech przedmiotu zamówienia zostały przez niego ściśle określone, żeby zapewnić taką samą jakość przedmiotu zamówienia w przypadku każdego wyłonionego w postępowaniu Wykonawcy. Przesłanką do zastosowania kryterium 100% ceny jest sam przedmiot zamówienia, który jest powszechnie dostępny na rynku oraz ma ustalone standardy jakościowe.
- 17.2. Zamawiający dokona oceny ofert, które nie zostały odrzucone, na podstawie następujących kryteriów oceny ofert dla każdej części zamówienia:

Lp.	Nazwa kryterium	Znaczenie kryterium (w %)
1	Cena	100

- 17.3. Ocena ofert zostanie dokonana oddzielnie dla każdej części.





- 17.4. Zamawiający dokona oceny ofert przyznając punkty w ramach poszczególnych kryteriów oceny ofert, przyjmując zasadę, że 1% = 1 punkt.
- 17.5. Kryterium cena będzie rozpatrywane na podstawie ceny brutto za wykonanie przedmiotu zamówienia, podanej przez Wykonawcę na Formularzu Oferty.
- 17.6. Punkty za kryterium „Cena” zostaną obliczone według wzoru:

$$P_c = \frac{C_n}{C_b} \times 100 \text{ pkt}$$

gdzie,

$P_c$  - ilość punktów za kryterium cena,

$C_n$  - najniższa cena ofertowa brutto spośród ofert nieodrzuconych,

$C_b$  – cena brutto oferty badanej.

W kryterium „Cena”, oferta z najniższą ceną brutto otrzyma 100 punktów a pozostałe oferty po matematycznym przeliczeniu w odniesieniu do najniższej ceny odpowiednio mniej. Końcowy wynik powyższego działania zostanie zaokrąglony do dwóch miejsc po przecinku.

- 17.7. Jako najkorzystniejszą zostanie wybrana oferta, która otrzyma największą ilość punktów, na podstawie kryteriów oceny ofert określonych w pkt 17.2,
- 17.8. Do wyboru najkorzystniejszej oferty są dopuszczone wyłącznie oferty uznane za ważne niepodlegające odrzuceniu.

## 18. WYBÓR NAJKORZYSTNIEJSZEJ OFERTY

- 18.1. Zamawiający wybiera najkorzystniejszą ofertę w terminie związania ofertą.
- 18.2. Jeżeli termin związania ofertą upłynął przed wyborem najkorzystniejszej oferty, Zamawiający wzywa Wykonawcę, którego oferta otrzymała najwyższą ocenę, do wyrażenia, w wyznaczonym przez Zamawiającego terminie, pisemnej zgody na wybór jego oferty.
- 18.3. Zamawiający niezwłocznie po wyborze najkorzystniejszej oferty informuje równocześnie Wykonawców, którzy złożyli oferty, o:
- 1) wyborze najkorzystniejszej oferty, podając nazwę albo imię i nazwisko, siedzibę albo miejsce zamieszkania, jeżeli jest miejscem wykonywania działalności Wykonawcy, którego ofertę wybrano, oraz nazwy albo imiona i nazwiska, siedziby albo miejsca zamieszkania, jeżeli są miejscami wykonywania działalności Wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację,
  - 2) Wykonawcach, których oferty zostały odrzucone.  
- podając uzasadnienie faktyczne i prawne.
- 18.4. Zamawiający udostępnia niezwłocznie informacje, o których mowa w pkt 18.3 ppkt 1SWZ na stronie internetowej prowadzonego postępowania.

## 19. INFORMACJE O FORMALNOŚCIACH, JAKIE MUSZĄ ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

- 19.1 W przypadku, gdy zostanie wybrana jako najkorzystniejsza oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Wykonawca przed podpisaniem umowy na wezwanie Zamawiającego przedłoży umowę regulującą współpracę Wykonawców.

- 19.2 Osoby reprezentujące Wykonawcę przy podpisywaniu umowy powinny posiadać ze sobą dokumenty potwierdzające ich umocowanie do reprezentowania Wykonawcy, o ile umocowanie to nie będzie wynikać z dokumentów załączonych do oferty.

## 20. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający **nie wymaga** zabezpieczenia należytego wykonania umowy.

## 21. PROJEKTOWANE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, KTÓRE ZOSTANĄ WPROWADZONE DO UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

21.1 Projekt Umowy stanowi **Załącznik Nr 2 do SWZ**.

21.2 Zamawiający przewiduje możliwości wprowadzenia zmian do zawartej umowy, na podstawie art. 454-455 ustawy Pzp oraz postanowień Projektu Umowy.

## 22. OCHRONA DANYCH OSOBOWYCH

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

1. Administratorem Pani/Pana danych osobowych jest **Gmina Potok Górny, reprezentowana przez Wójta Gminy z siedzibą mieszczącą się pod adresem: Potok Górny 116, 23-423 Potok Górny, telefon kontaktowy: 84 685-25-00 – zwanego dalej „Administratorem” lub „Zamawiającym**
2. W sprawach z zakresu ochrony danych osobowych mogą Państwo kontaktować się z Inspektorem Ochrony Danych pod adresem e-mail: **iod@potokgorny.com.pl**
3. Pani/Pana dane osobowe będą przetwarzane w celu związanym z postępowaniem o udzielenie zamówienia publicznego pn. **„Zakup sprzętu IT wraz z oprogramowaniem w ramach projektu Zwiększenie cyberbezpieczeństwa Gminy Potok Górny”**.
4. Dane osobowe będą przetwarzane przez okres zgodnie z art. 78 ust. 1 i 4 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t. j. Dz. U. z 2022 r. poz. 1710 z późn. zm.), zwanej dalej PZP, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas obowiązywania umowy.
5. Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. c) ww. Rozporządzenia w związku z przepisami PZP.
6. Odbiorcami Pani/Pana danych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 4 PZP.
7. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach PZP, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z PZP.
8. Osoba, której dane dotyczą ma prawo do:

- dostępu do treści swoich danych oraz możliwości ich poprawiania, sprostowania, ograniczenia przetwarzania,
- w przypadku gdy przetwarzanie danych odbywa się z naruszeniem przepisów Rozporządzenia służy prawo wniesienia skargi do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa,

**9. Osobie, której dane dotyczą nie przysługuje:**

- w związku z art. 17 ust. 3 lit. b, d lub e Rozporządzenia prawo do usunięcia danych osobowych;
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 Rozporządzenia;
- na podstawie art. 21 Rozporządzenia prawo sprzeciwu, wobec przetwarzania danych osobowych.

**10.** W przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1-3 Rozporządzenia, wymagałoby niewspółmiernie dużego wysiłku, Administrator może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego.

**11.** Skorzystanie przez osobę, której dane dotyczą, z uprawnienia do sprostowania lub uzupełnienia danych osobowych, o którym mowa w art. 16 Rozporządzenia, nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego lub konkursu ani zmianą postanowień umowy w zakresie niezgodnym z PZP.

**12.** Wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 Rozporządzenia, nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia publicznego.

**13.** W przypadku danych osobowych zamieszczonych przez Administratora w Biuletynie Zamówień Publicznych, prawa, o których mowa w art. 15 i art. 16 Rozporządzenia, są wykonywane w drodze żądania skierowanego do Administratora.

**14.** Od dnia zakończenia postępowania o udzielenie zamówienia, w przypadku gdy wniesienie żądania, o którym mowa w art. 18 ust. 1 Rozporządzenia, spowoduje ograniczenie przetwarzania danych osobowych zawartych w protokole i załącznikach do protokołu, Administrator nie udostępnia tych danych zawartych w protokole i w załącznikach do protokołu, chyba że zachodzą przesłanki, o których mowa w art. 18 ust. 2 Rozporządzenia.

**15.** W przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1-3 Rozporządzenia, wymagałoby niewspółmiernie dużego wysiłku, Administrator może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających w szczególności na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia.

**16.** Skorzystanie przez osobę, której dane dotyczą, z uprawnienia do sprostowania lub uzupełnienia, o którym mowa w art. 16 Rozporządzenia, nie może naruszać integralności protokołu oraz jego załączników.

**17.** Ponadto informujemy, iż w związku z przetwarzaniem Pani/Pana danych osobowych nie podlega Pan/Pani decyzjom, które się opierają wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, o czym stanowi art. 22 Rozporządzenia.

## **23. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ**

**23.1** Środki ochrony prawnej przewidziane są w dziale IX ustawy Pzp

**23.2** Środkami ochrony prawnej są odwołanie i skarga do sądu.



**23.3** Środki ochrony prawnej przysługują wykonawcy oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 ustawy Pzp oraz Rzecznikowi Małych i Średnich Przedsiębiorców.

**23.4** 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;

**23.5** Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej. Odwołujący przekazuje zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, że zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przekazanie odpowiednio odwołania albo jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.

**23.6** Terminy wnoszenia odwołań:

1. Odwołanie wnosi się w terminie:

- a) 5 dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,
- b) 10 dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w lit. a.

2. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub konkurs lub wobec treści dokumentów zamówienia wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub dokumentów zamówienia na stronie internetowej.

3. Odwołanie w przypadkach innych niż określone w pkt 1 i 2 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.

4. Jeżeli Zamawiający nie przesłał Wykonawcy zawiadomienia o wyborze oferty najkorzystniejszej odwołanie wnosi się nie później niż w terminie:

- 1) 15 dni od dnia zamieszczenia w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania
- 2) miesiąca od dnia zawarcia umowy, jeżeli Zamawiający nie zamieścił w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania.

**23.7** Odwołanie zawiera:

- 1) imię i nazwisko albo nazwę, miejsce zamieszkania albo siedzibę, numer telefonu oraz adres poczty elektronicznej odwołującego oraz imię i nazwisko przedstawiciela (przedstawicieli);
- 2) nazwę i siedzibę zamawiającego, numer telefonu oraz adres poczty elektronicznej zamawiającego;

- 3) numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub NIP odwołującego będącego osobą fizyczną, jeżeli jest on obowiązany do jego posiadania albo posiada go nie mając takiego obowiązku;
- 4) numer w Krajowym Rejestrze Sądowym, a w przypadku jego braku - numer w innym właściwym rejestrze, ewidencji lub NIP odwołującego niebędącego osobą fizyczną, który nie ma obowiązku wpisu we właściwym rejestrze lub ewidencji, jeżeli jest on obowiązany do jego posiadania;
- 5) określenie przedmiotu zamówienia;
- 6) wskazanie numeru ogłoszenia w przypadku zamieszczenia w Biuletynie Zamówień Publicznych
- 7) wskazanie czynności lub zaniechania czynności zamawiającego, której zarzuca się niezgodność z przepisami ustawy, lub wskazanie zaniechania przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy;
- 8) zwięzłe przedstawienie zarzutów;
- 9) żądanie co do sposobu rozstrzygnięcia odwołania;
- 10) wskazanie okoliczności faktycznych i prawnych uzasadniających wniesienie odwołania oraz dowodów na poparcie przytoczonych okoliczności;
- 11) podpis odwołującego albo jego przedstawiciela lub przedstawicieli;
- 12) wykaz załączników.

Do odwołania dołącza się:

- 1) dowód uiszczenia wpisu od odwołania w wymaganej wysokości;
  - 2) dowód przekazania odpowiednio odwołania albo jego kopii zamawiającemu;
  - 3) dokument potwierdzający umocowanie do reprezentowania odwołującego.
- 23.8 Na orzeczenie Izby stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargę wnosi się do Sądu Okręgowego w Warszawie - sądu zamówień publicznych.

## 24. KLAUZULA ZATRUDNIENIA

W związku z tym, że postępowanie prowadzone jest wg przepisów dla dostaw nie obowiązuje art. 95 ust. 1 ustawy Pzp.

## 24. INFORMACJE DODATKOWE

- 25.1 Zamawiający **nie dopuszcza** składania ofert częściowych.
- 25.2 Zamawiający **nie dopuszcza** składania ofert wariantowych.
- 25.3 Zamawiający **nie przewiduje** wymagań wskazanych w art. 96 ust. 2 pkt 2 ustawy Pzp.
- 25.4 Zamawiający **nie przewiduje** zamówień, o których mowa w art. 214 ust. 1 pkt 7 i 8 ustawy Pzp.
- 25.5 Zamawiający **nie wymaga** przeprowadzenia przez Wykonawcę wizji lokalnej lub sprawdzenia przez niego dokumentów niezbędnych do realizacji zamówienia, o których mowa w art. 131 ust. 2 ustawy Pzp.
- 25.6 Zamawiający **nie przewiduje** rozliczenia między Zamawiającym a Wykonawcą w walutach obcych.



- 25.7 Zamawiający **nie przewiduje** zwrotu kosztów udziału w postępowaniu.
- 25.8 Zamawiający **nie wymaga** obowiązku osobistego wykonania przez Wykonawcę kluczowych zadań zgodnie z art. 60 i art. 121 ustawy Pzp.
- 25.9 Zamawiający **nie przewiduje** zawarcia umowy ramowej.
- 25.10 Zamawiający **nie przewiduje** wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej wraz z informacjami, o których mowa w art. 230 ustawy Pzp.
- 25.11 Zamawiający **nie stawia** wymogu lub możliwości złożenia ofert w postaci katalogów elektronicznych lub dołączenia katalogów elektronicznych do oferty, w sytuacji określonej w art. 93 ustawy Pzp.

## 25. ZAŁĄCZNIKI DO SWZ

Integralną częścią SWZ są załączniki:

- Załącznik Nr 1 – Szczegółowy Opis Przedmiotu Zamówienia,
- Załącznik Nr 2 – Projekt umowy.
- Załącznik Nr 3 – Wzór Formularza ofertowego.
- Załącznik Nr 4 - Wzór oświadczenia wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia składanego na podstawie art. 125 ust. 1 ustawy Pzp.
- Załącznik Nr 5 - Wzór oświadczenia podmiotu udostępniającego zasoby składanego na podstawie art. 125 ust. 1 ustawy Pzp
- Załącznik Nr 6 – Wzór oświadczenia Wykonawców wspólnie ubiegających się o udzielenie zamówienia,,
- Załącznik Nr 7 – Wzór wykazu wykonanych usług
- Załącznik Nr 8 - Opis charakterystyki zaoferowanego sprzętu informatycznego i oprogramowania,



## SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

### „Zakup sprzętu IT wraz z oprogramowaniem w ramach projektu Zwiększenie cyberbezpieczeństwa Gminy Potok Górny”

Dostawa fabrycznie nowego sprzętu do Urzędu Gminy w Potoku Górnym, 23-423 Potok Górny 116 o wskazanych poniżej lub równoważnych parametrach i funkcjach technicznych nie gorszych niż wskazane.

**W ofercie należy podać nazwę producenta, typ, model, oferowanego sprzętu umożliwiającą jednoznaczną identyfikację oferowanej konfiguracji.**

Nie dopuszcza się modyfikacji na drodze Producent-Zamawiający (np. modyfikacji lub wymiany jakiegokolwiek komponentu sprzętowego).

Zakres zadania obejmuje w szczególności

Lp.	Nazwa	Ilość
<b>Część 1 Dostawa serwerów z oprogramowaniem</b>		
1.	Zakup serwera z oprogramowaniem typ I	1 szt.
2.	Zakup serwera z oprogramowaniem typ II	1 szt.
3.	Zakup i wdrożenie rozwiązania Network Access Control	1 kpl.
4.	Zakup oprogramowania do archiwizacji i kategoryzacji logów	1 kpl.
5.	Zakup oprogramowania do inwentaryzacji i ochrony przed wyciekiem DLP	1 kpl.
<b>Część 2 Dostawa przełączników sieciowych, serwera NAS oraz UPS - a</b>		
6.	Zakup serwer NAS	2 szt.
7.	Zakup przełącznika sieciowego zarządzalnego	3 szt.
8.	Zakup UPS	1 kpl.

### Wymagania ogólne.

1. Dostarczony sprzęt i oprogramowanie muszą być wolne od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt i oprogramowanie muszą być fabrycznie nowe (tzn. wyprodukowane nie wcześniej, niż na 12 miesięcy przed ich dostarczeniem), muszą pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu i oprogramowania.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale”, „end-of-support”, „end-of-life” producenta lub innych listach prowadzonych przez producentów produktów świadczących o tym, że produkt został wycofany ze sprzedaży, wsparcie dla niego zostało zakończone lub producent zaprzestaje wydawania aktualizacji, poprawek bezpieczeństwa czy też napraw dla produktu.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów. Niedopuszczalna jest realizacja tylko części funkcji bądź wymaganych standardów zamiast innych określonych jako minimalne w niniejszym dokumencie. Wszystkie wymagania minimalne muszą zostać zapewnione przez dostarczane produkty bez

konieczności zakupu żadnych dodatkowych elementów przez Zamawiającego, chyba że z niniejszego dokumentu wynika inaczej.

5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do wskazanej przez Zamawiającego lokalizacji.
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzeń do działania, pozwalające na rozpoczęcie pracy oraz dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.
8. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
9. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
10. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
11. Dla dostaw sprzętu informatycznego z oprogramowaniem Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania (w tym systemu operacyjnego) nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania (faktury, rachunki) w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
12. Dla dostaw oprogramowania Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania, nieużywanego oraz nigdy wcześniej nieaktywowanego oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania posiadającego fizyczny nośnik naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

W poniższych tabelach przedstawiono minimalne wymagania w zakresie specyfikacji technicznej poszczególnych pozycji.

## 1 ZAKUP SERWERA Z OPROGRAMOWANIEM TYP I- 1 KPL.

L.p	Parametr	Charakterystyka (wymagania minimalne)
1.	Obudowa	<ul style="list-style-type: none"> <li>- Obudowa Rack o wysokości 1U.</li> <li>- 8 wnęk na dyski 2.5".</li> <li>- Możliwość instalacji dysków SAS/SATA/M.2 – Fabryczna blokada demontowania dysków twardych zamykana na klucz lub za pomocą zamka lub innego podobnego zabezpieczenia.</li> <li>- LCD na froncie obudowy lub diody LED informujące o stanie komponentów np. CPU, RAM, SSD, zasilanie.</li> </ul>
2.	Płyta główna	<ul style="list-style-type: none"> <li>- Płyta główna z możliwością zainstalowania jednego procesora.</li> <li>- Obsługa procesorów 144 rdzeniowych.</li> <li>- Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.</li> <li>- Na płycie głównej powinny znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.</li> <li>- Płyta główna powinna obsługiwać do 4TB pamięci RAM.</li> </ul>
3.	Procesor	<ul style="list-style-type: none"> <li>- Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych.</li> <li>- Zainstalowany jeden procesor min. 12-rdzeniowy, klasy x86 dedykowany do pracy z zaferowanym serwerem umożliwiającym osiągnięcie wyniku min. 140 w teście SPECspeed@2017_fp_base, dostępnym na stronie <a href="http://www.spec.org">www.spec.org</a> dla konfiguracji jednoprocessorowej oferowanego serwera</li> </ul>
4.	RAM	<ul style="list-style-type: none"> <li>- 64 GB DDR5 RDIMM.</li> <li>- Pamięć RAM musi wspierać wczesne wykrywanie błędów poprawialnych (CE) w pamięci i przeprowadzanie operacji izolacji. Pamięć musi wspierać typowe technologie ochrony m.in. ECC, Address/Command Parity, PPR, Write Data CRC Protection, ADC-SR, ADDDC-MR, SDDC.</li> </ul>
5.	Kontroler RAID	<ul style="list-style-type: none"> <li>- Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID 0, 1, 10, 5, 6, 60.</li> </ul>
6.	Dyski twarde	<ul style="list-style-type: none"> <li>- Zainstalowane min. 3 dyski 2,5-calowe: <ul style="list-style-type: none"> <li>o 2 x 1,9 TB minimum (HDD, 10000 obr./min, SAS 12 Gb/s, 2.5", Hot-Plug)</li> <li>o 1 x 480 GB minimum (SSD, SATA 6 Gb/s, 2.5", Hot-Plug)</li> </ul> </li> <li>- Możliwość zainstalowania dwóch dysków M.2 SSD o pojemności 480GB Hot-Plug z możliwością konfiguracji RAID 1.</li> </ul>
7.	Gniazda PCIe	<ul style="list-style-type: none"> <li>- 2x PCIe 4.0 x16</li> </ul>
8.	Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> <li>- Min. 2 interfejsy sieciowe 1GbE BASE-T</li> <li>- Min. 2 interfejsy sieciowe SFP+ 10GbE</li> </ul>
9.	Wbudowane porty oraz wskaźniki	<ul style="list-style-type: none"> <li>- 3 porty USB w tym min: <ul style="list-style-type: none"> <li>o 1 port USB 3.1,</li> <li>o 1 port USB z przodu obudowy</li> <li>o 1 port USB 2.0 Type-C</li> </ul> </li> <li>- 1 port VGA</li> </ul>
10.	Video	<ul style="list-style-type: none"> <li>- Zintegrowana karta graficzna osiągająca rozdzielczość 1920x1200</li> </ul>
11.	Wentylatory	<ul style="list-style-type: none"> <li>- Redundantne</li> </ul>
12.	Zasilacze	<ul style="list-style-type: none"> <li>- Minimum dwa redundantne zasilacze każdy o mocy zapewniającej prawidłową pracę serwera, moc minimum 800W</li> </ul>
13.	Elementy montażowe	<ul style="list-style-type: none"> <li>- Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych</li> </ul>
14.	Bezpieczeństwo	<ul style="list-style-type: none"> <li>- Moduł TPM 2.0</li> <li>- Secure boot</li> <li>- Ochrona przed atakami. Urządzenie musi udostępniać minimalną wymaganą liczbę portów usług sieciowych. Domyślnie, zbędne usługi muszą być wyłączone, porty usług sieciowych do debugowania i diagnozy muszą być wyłączone podczas normalnej pracy serwera.</li> </ul>



15.	<b>BIOS</b>	<ul style="list-style-type: none"> <li>- Oferowany serwer musi być wyposażony w BIOS zapewniający następujące funkcjonalności: <ul style="list-style-type: none"> <li>o Inicjalizacja sprzętu: BIOS musi wspierać pełne testowanie i uruchamianie kluczowych komponentów serwera, takich jak procesory, pamięć RAM, dyski twarde oraz interfejsy sieciowe.</li> <li>o Zarządzanie konfiguracją systemu: BIOS musi umożliwiać konfigurację ustawień systemowych, w tym kolejności bootowania, konfiguracji RAID oraz ustawień zasilania.</li> <li>o Bezpieczeństwo systemu: BIOS musi wspierać funkcję Secure Boot, chroniącą przed uruchamianiem nieautoryzowanego oprogramowania. Musi również posiadać opcję zabezpieczenia hasłem dostępu.</li> </ul> </li> <li>- Aktualizacje oprogramowania: BIOS musi umożliwiać aktualizację firmware'u oraz zapewniać wsparcie dla aktualizacji zdalnych.</li> </ul>
16.	<b>Bezpieczeństwo</b>	<ul style="list-style-type: none"> <li>- Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania.</li> <li>- Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</li> <li>- BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła</li> <li>- Moduł TPM 2.0</li> <li>- Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera</li> <li>- Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem</li> <li>- Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155.</li> </ul>
17.	<b>Karta Zarządzania</b>	<ul style="list-style-type: none"> <li>- Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające:</li> <li>- zdalny dostęp do graficznego interfejsu Web karty zarządzającej</li> <li>- szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika</li> <li>- możliwość podmontowania zdalnych wirtualnych napędów</li> <li>- wirtualną konsolę z dostępem do myszy, klawiatury</li> <li>- wsparcie dla IPv6</li> <li>- wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH</li> <li>- integracja z Active Directory</li> <li>- możliwość obsługi przez trzech administratorów jednocześnie</li> <li>- Wsparcie dla automatycznej rejestracji DNS</li> <li>- wsparcie dla LLDP</li> <li>- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej</li> <li>- możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy.</li> <li>- Monitorowanie zużycia dysków SSD</li> <li>- Automatyczne update firmware dla wszystkich komponentów serwera</li> <li>- Możliwość przywrócenia poprzednich wersji firmware</li> <li>- Możliwość eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, konfiguracji kontrolera RAID) serwera do pliku XML lub JSON lub innego</li> <li>- Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych</li> <li>- Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram.</li> <li>- kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania</li> </ul>
18.	<b>Oprogramowanie do zarządzania</b>	<ul style="list-style-type: none"> <li>- Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:</li> <li>- integracja z Active Directory</li> </ul>

		<ul style="list-style-type: none"> <li>- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta</li> <li>- Wsparcie dla protokołów SNMP, IPMI, Linux SSH,</li> <li>- Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram</li> <li>- Szczegółowy opis wykrytych systemów oraz ich komponentów</li> <li>- Możliwość eksportu raportu do CSV, HTML, XLS, PDF</li> <li>- Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.</li> <li>- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach</li> <li>- Szybki podgląd stanu środowiska</li> <li>- Podsumowanie stanu dla każdego urządzenia</li> <li>- Szczegółowy status urządzenia/elementu/komponentu</li> <li>- Generowanie alertów przy zmianie stanu urządzenia.</li> <li>- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń</li> <li>- Możliwość przejęcia zdalnego pulpitu</li> <li>- Możliwość podmontowania wirtualnego napędu</li> <li>- Kreator umożliwiający dostosowanie akcji dla wybranych alertów</li> <li>- Przesyłanie alertów „as-is” do innych konsol firm trzecich</li> <li>- Możliwość definiowania ról administratorów</li> <li>- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów</li> <li>- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)</li> <li>- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta</li> <li>- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informacje o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.</li> <li>- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.</li> <li>- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.</li> <li>- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.</li> <li>- Zdalne uruchamianie diagnostyki serwera.</li> <li>- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.</li> </ul>
19.	Oprogramowanie do monitorowania	<ul style="list-style-type: none"> <li>- Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</li> <li>- Monitoring:</li> <li>- ilość podłączonych oraz rozłączonych systemów</li> <li>- stan podłączonych urządzeń</li> <li>- informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów</li> <li>- Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia</li> <li>- informacje o statusie gwarancji dla poszczególnych urządzeń</li> <li>- informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń</li> <li>- Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych</li> <li>- Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących.</li> <li>- Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.</li> <li>- Monitoring parametrów serwerów z informacją o minimum:</li> </ul>

		<ul style="list-style-type: none"> <li>- Obciążeniu procesora</li> <li>- Zużyciu pamięci RAM</li> <li>- Temperaturze procesorów</li> <li>- Zmianach w fizycznej konfiguracji serwera</li> <li>- Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.</li> <li>- Aktualizacja firmware</li> <li>- możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania</li> <li>- Raporty</li> <li>- Możliwość generowania raportów dla serwerów zawierających informację o:</li> <li>- Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej</li> <li>- Średnim obciążeniu: procesorów, pamięci RAM, IO,</li> <li>- Generowanie raportów do plików CSV i PDF</li> <li>- Cyberbezpieczeństwo</li> <li>- Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.</li> <li>- Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce.</li> <li>- Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.</li> <li>- Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.</li> </ul>	
20.	Certyfikaty	<ul style="list-style-type: none"> <li>- Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent serwera opracował, wdrożył i certyfikował system zarządzania jakością;</li> <li>- Certyfikat ISO 50001 lub Certyfikat ISO 14001 lub inny równoważny dokument poświadczający, że producent serwera posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność;</li> <li>- Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany serwer spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE;</li> <li>- Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych.</li> <li>- Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.</li> </ul>	
21.	System operacyjny/dodatkowe oprogramowanie	<ul style="list-style-type: none"> <li>- Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego klasy Microsoft Windows Serwer Standard w najnowszej dostępnej wersji oferowanej przez producenta oprogramowania umożliwiającego uruchomienie serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.</li> <li>- Warunki równoważności dla dostawy oprogramowania Microsoft Windows Serwer Standard w najnowszej wersji oferowanej przez producenta oprogramowania: <ul style="list-style-type: none"> <li>a) Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji oraz dostępu do serwerowego systemu operacyjnego.</li> <li>b) Możliwość wykorzystywania 248 procesorów wirtualnych oraz 24TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy</li> </ul> </li> </ul>	



		<p>system operacyjny.</p> <p>c) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.</p> <p>d) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.</p> <p>e) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.</p> <p>f) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.</p> <p>g) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.</p> <p>h) Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;</p> <p>i) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</p> <p>j) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.</p> <p>k) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.</p> <p>l) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.</p> <p>m) Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</p> <p>n) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.</p> <p>o) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.</p> <p>p) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play).</p> <p>q) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</p> <p>r) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).</p> <p>s) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.</p> <p>t) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</p> <p>u) Co najmniej 10 lat wsparcia długoterminowego.</p> <p>v) Wsparcie protokołu SMB za pośrednictwem rozwiązania QUIC.</p>	
22.	<b>Licencje dostępne</b>	25 Licencji dostępowych uprawniających na korzystanie z usług serwera. Licencja „na użytkownika”	
23.	<b>Dokumentacja użytkownika</b>	<ul style="list-style-type: none"> <li>- Zamawiający wymaga dokumentacji w języku polskim lub angielskim oraz dostęp do oprogramowania wymaganego do poprawnego funkcjonowania serwera.</li> <li>- Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</li> <li>- Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia</li> </ul>	
24.	<b>Warunki serwisu i gwarancji</b>	<ul style="list-style-type: none"> <li>- Gwarancja: min. 24 miesiące gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dysków Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii w języku polskim poprzez ogólnopolską linię telefoniczną producenta oraz dedykowany portal techniczny producenta, dla obu kanałów w trybie ciągłym, tj. niezależnie od pory dnia, dni roboczych i dni wolnych od pracy</li> <li>- Zamawiający wymaga przynajmniej dwóch podstawowych form kontaktu serwisowego tj. całodobowej infolinii oraz formularza online.</li> </ul>	

		<ul style="list-style-type: none"> <li>- Oferowane wsparcie musi być świadczone w języku polskim bezpośrednio przez Producenta.</li> <li>- Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.</li> <li>- Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</li> <li>- Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.</li> <li>- w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego</li> </ul>	
25.	Wsparcie serwisowe	W przypadku jeżeli serwis gwarancyjny urządzeń nie będzie realizowany bezpośrednio przez producenta urządzenia, wówczas firma serwisująca musi posiadać certyfikat ISO 9001 oraz ISO 27001 lub inny równoważny dokument poświadczający, że usługi serwisu świadczone będą zgodnie z zasadami wynikającymi z tych norm oraz firma serwisująca musi posiadać autoryzację producenta urządzeń.	

## 2 ZAKUP SERWERA Z OPROGRAMOWANIEM TYP II- 1 KPL.

L.p	Parametr	Charakterystyka (wymagania minimalne)	
1.	Obudowa	<ul style="list-style-type: none"> <li>- Obudowa Rack o wysokości 1U.</li> <li>- 8 wnęk na dyski 2.5".</li> <li>- Możliwość instalacji dysków SAS/SATA/M.2 – Fabryczna blokada demontowania dysków twardych zamykana na klucz lub za pomocą zamka lub innego podobnego zabezpieczenia.</li> <li>- LCD na froncie obudowy lub diody LED informujące o stanie komponentów np. CPU, RAM, SSD, zasilanie.</li> </ul>	
2.	Płyta główna	<ul style="list-style-type: none"> <li>- Płyta główna z możliwością zainstalowania jednego procesora.</li> <li>- Obsługa procesorów 144 rdzeniowych.</li> <li>- Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.</li> <li>- Na płycie głównej powinny znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.</li> <li>- Płyta główna powinna obsługiwać do 4TB pamięci RAM.</li> </ul>	
3.	Procesor	<ul style="list-style-type: none"> <li>- Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych.</li> <li>- Zainstalowany jeden procesor min. 8-rdzeniowy, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 80 w teście SPECspeed@2017_fp_base, dostępnym na stronie <a href="http://www.spec.org">www.spec.org</a> dla konfiguracji jednoprocessorowej oferowanego serwera – wyniki testu załączyć do oferty.</li> </ul>	
4.	RAM	<ul style="list-style-type: none"> <li>- 32 GB DDR5 RDIMM.</li> <li>- Pamięć RAM musi wspierać wczesne wykrywanie błędów poprawialnych (CE) w pamięci i przeprowadzanie operacji izolacji. Pamięć musi wspierać typowe technologie ochrony m.in. ECC, Address/Command Parity, PPR, Write Data CRC Protection, ADC-SR, ADDDC-MR, SDDC.</li> </ul>	
5.	Kontroler RAID	<ul style="list-style-type: none"> <li>- Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID 0, 1, 10, 5, 6, 60.</li> </ul>	
6.	Dyski twarde	<ul style="list-style-type: none"> <li>- Zainstalowane min. 3 dyski 2,5-calowe: <ul style="list-style-type: none"> <li>o 2 x 1,9 TB minimum (HDD, 10000 obr./min, SAS 12 Gb/s, 2.5", Hot-Plug)</li> <li>o 1 x 480 GB minimum (SSD, SATA 6 Gb/s, 2.5", Hot-Plug)</li> </ul> </li> <li>- Możliwość zainstalowania dwóch dysków M.2 SSD o pojemności 480GB Hot-Plug z</li> </ul>	

		możliwością konfiguracji RAID 1.	
7.	<b>Gniazda PCIe</b>	- 2x PCIe 4.0 x16	
8.	<b>Interfejsy sieciowe/FC/SAS</b>	- Min. 2 interfejsy sieciowe 1GbE BASE-T - Min. 2 interfejsy sieciowe SFP+ 10GbE	
9.	<b>Wbudowane porty oraz wskaźniki</b>	- 3 porty USB w tym min: o 1 port USB 3.1, o 1 port USB z przodu obudowy o 1 port USB 2.0 Type-C - 1 port VGA	
10.	<b>Video</b>	- Zintegrowana karta graficzna osiągająca rozdzielczość 1920x1200	
11.	<b>Wentylatory</b>	- Redundantne	
12.	<b>Zasilacze</b>	- Minimum dwa redundantne zasilacze każdy o mocy zapewniającej prawidłową pracę serwera, moc minimum 700W	
13.	<b>Elementy montażowe</b>	- Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych	
14.	<b>Bezpieczeństwo</b>	- Moduł TPM 2.0 - Secure boot - Ochrona przed atakami. Urządzenie musi udostępniać minimalną wymaganą liczbę portów usług sieciowych. Domyślnie, zbędne usługi muszą być wyłączone, porty usług sieciowych do debugowania i diagnozy muszą być wyłączone podczas normalnej pracy serwera.	
15.	<b>BIOS</b>	- Oferowany serwer musi być wyposażony w BIOS zapewniający następujące funkcjonalności: o Inicjalizacja sprzętu: BIOS musi wspierać pełne testowanie i uruchamianie kluczowych komponentów serwera, takich jak procesory, pamięć RAM, dyski twarde oraz interfejsy sieciowe. o Zarządzanie konfiguracją systemu: BIOS musi umożliwiać konfigurację ustawień systemowych, w tym kolejności bootowania, konfiguracji RAID oraz ustawień zasilania. o Bezpieczeństwo systemu: BIOS musi wspierać funkcję Secure Boot, chroniącą przed uruchamianiem nieautoryzowanego oprogramowania. Musi również posiadać opcję zabezpieczenia hasłem dostępu. - Aktualizacje oprogramowania: BIOS musi umożliwiać aktualizację firmware'u oraz zapewniać wsparcie dla aktualizacji zdalnych.	
16.	<b>Bezpieczeństwo</b>	- Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. - Możliwość wyłączenia w BIOS funkcji przycisku zasilania. - BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła - Moduł TPM 2.0 - Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera - Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem - Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155.	
17.	<b>Karta Zarządzania</b>	- Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej - szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika - możliwość podmontowania zdalnych wirtualnych napędów - wirtualną konsolę z dostępem do myszy, klawiatury - wsparcie dla IPv6 - wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH	



		<ul style="list-style-type: none"> <li>- integracja z Active Directory</li> <li>- możliwość obsługi przez trzech administratorów jednocześnie</li> <li>- Wsparcie dla automatycznej rejestracji DNS</li> <li>- wsparcie dla LLDP</li> <li>- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej</li> <li>- możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy.</li> <li>- Monitorowanie zużycia dysków SSD</li> <li>- Automatyczne update firmware dla wszystkich komponentów serwera</li> <li>- Możliwość przywrócenia poprzednich wersji firmware</li> <li>- Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, konfiguracji kontrolera RAID) serwera do pliku XML lub JSON lub innego</li> <li>- Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych</li> <li>- Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.</li> <li>- kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania</li> </ul>	
18.	Oprogramowanie do zarządzania	<ul style="list-style-type: none"> <li>- Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:</li> <li>- integracja z Active Directory</li> <li>- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta</li> <li>- Wsparcie dla protokołów SNMP, IPMI, Linux SSH,</li> <li>- Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram</li> <li>- Szczegółowy opis wykrytych systemów oraz ich komponentów</li> <li>- Możliwość eksportu raportu do CSV, HTML, XLS, PDF</li> <li>- Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.</li> <li>- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach</li> <li>- Szybki podgląd stanu środowiska</li> <li>- Podsumowanie stanu dla każdego urządzenia</li> <li>- Szczegółowy status urządzenia/elementu/komponentu</li> <li>- Generowanie alertów przy zmianie stanu urządzenia.</li> <li>- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń</li> <li>- Możliwość przejęcia zdalnego pulpitu</li> <li>- Możliwość podmontowania wirtualnego napędu</li> <li>- Kreator umożliwiający dostosowanie akcji dla wybranych alertów</li> <li>- Przesyłanie alertów „as-is” do innych konsol firm trzecich</li> <li>- Możliwość definiowania ról administratorów</li> <li>- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów</li> <li>- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)</li> <li>- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta</li> <li>- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.</li> <li>- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.</li> <li>- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.</li> <li>- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.</li> </ul>	

		<ul style="list-style-type: none"> <li>- Zdalne uruchamianie diagnostyki serwera.</li> <li>- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.</li> </ul>	
19.	<b>Oprogramowanie do monitorowania</b>	<ul style="list-style-type: none"> <li>- Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</li> <li>- Monitoring:</li> <li>- ilość podłączonych oraz rozłączonych systemów</li> <li>- stan podłączonych urządzeń</li> <li>- informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów</li> <li>- Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia</li> <li>- informacje o statusie gwarancji dla poszczególnych urządzeń</li> <li>- informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń</li> <li>- Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych</li> <li>- Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących.</li> <li>- Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.</li> <li>- Monitoring parametrów serwerów z informacją o minimum:</li> <li>- Obciążeniu procesora</li> <li>- Zużyciu pamięci RAM</li> <li>- Temperaturze procesorów</li> <li>- Zmianach w fizycznej konfiguracji serwera</li> <li>- Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliiach.</li> <li>- Aktualizacja firmware</li> <li>- możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania</li> <li>- Raporty</li> <li>- Możliwość generowania raportów dla serwerów zawierających informację o:</li> <li>- Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej</li> <li>- Średnim obciążeniu: procesorów, pamięci RAM, IO,</li> <li>- Generowanie raportów do plików CSV i PDF</li> <li>- Cyberbezpieczeństwo</li> <li>- Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.</li> <li>- Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce.</li> <li>- Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.</li> <li>- Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.</li> </ul>	
20.	<b>Certyfikaty</b>	<ul style="list-style-type: none"> <li>- Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent serwera opracował, wdrożył i certyfikował system zarządzania jakością;</li> <li>- Certyfikat ISO 50001 lub Certyfikat ISO 14001 lub inny równoważny dokument poświadczający, że producent serwera posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność;</li> <li>- Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany serwer spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE;</li> <li>- Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z</li> </ul>	

		<p>dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. - Wykonawca złoży dokument potwierdzający spełnianie wymogu</p> <ul style="list-style-type: none"> <li>- Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.</li> </ul>	
21.	<b>System operacyjny/dodatkowe oprogramowanie</b>	<ul style="list-style-type: none"> <li>- Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego klasy Microsoft Windows Server Standard w najnowszej dostępnej wersji oferowanej przez producenta oprogramowania umożliwiającego uruchomienie serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.</li> <li>- Warunki równoważności dla dostawy oprogramowania Microsoft Windows Server Standard w najnowszej wersji oferowanej przez producenta oprogramowania: <ul style="list-style-type: none"> <li>w) Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji oraz dostępu do serwerowego systemu operacyjnego.</li> <li>x) Możliwość wykorzystywania 248 procesorów wirtualnych oraz 24TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.</li> <li>y) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.</li> <li>z) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.</li> <li>aa) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.</li> <li>bb) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.</li> <li>cc) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.</li> <li>dd) Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;</li> <li>ee) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</li> <li>ff) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.</li> <li>gg) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.</li> <li>hh) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.</li> <li>ii) Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</li> <li>jj) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.</li> <li>kk) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.</li> <li>ll) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play).</li> <li>mm) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</li> <li>nn) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).</li> <li>oo) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.</li> </ul> </li> </ul>	



## Załącznik Nr 1

		<p>pp) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</p> <p>qq) Co najmniej 10 lat wsparcia długoterminowego.</p> <p>rr) Wsparcie protokołu SMB za pośrednictwem rozwiązania QUIC.</p>	
22.	<b>Licencje dostępne</b>	10 Licencji dostępowych uprawniających na korzystanie z usług serwera. Licencja na użytkownika	
23.	<b>Dokumentacja użytkownika</b>	<ul style="list-style-type: none"> <li>- Zamawiający wymaga dokumentacji w języku polskim lub angielskim oraz dostęp do oprogramowania wymaganego do poprawnego funkcjonowania serwera.</li> <li>- Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</li> <li>- Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia</li> </ul>	
24.	<b>Warunki serwisu i gwarancji</b>	<ul style="list-style-type: none"> <li>- Gwarancja: min. 24 miesiące gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dysków Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii w języku polskim poprzez ogólnopolską linię telefoniczną producenta oraz dedykowany portal techniczny producenta, dla obu kanałów w trybie ciągłym, tj. niezależnie od pory dnia, dni roboczych i dni wolnych od pracy</li> <li>- Zamawiający wymaga przynajmniej dwóch podstawowych form kontaktu serwisowego tj. całodobowej infolinii oraz formularza online.</li> <li>- Oferowane wsparcie musi być świadczone w języku polskim bezpośrednio przez Producenta.</li> <li>- Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.</li> <li>- Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</li> <li>- Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.</li> <li>- w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego</li> </ul>	
25.	<b>Wsparcie serwisowe</b>	W przypadku jeżeli serwis gwarancyjny urządzeń nie będzie realizowany bezpośrednio przez producenta urządzenia, wówczas firma serwisująca musi posiadać certyfikat ISO 9001 oraz ISO 27001 lub inny równoważny dokument poświadczający, że usługi serwisu świadczone będą zgodnie z zasadami wynikającymi z tych norm oraz firma serwisująca musi posiadać autoryzację producenta urządzeń.	

### 3 ZAKUP I WDROŻENIE ROZWIĄZANIA NETWORK ACCESS CONTROL- 110 IP

L.P	Parametr	Charakterystyka (wymagania minimalne)	
1.	Dane producenta /model	Producent oferowanego rozwiązania /model i wersja modelu	
2.	Opis funkcjonalności rozwiązania	Wymagane jest dostarczenie rozwiązania typu NAC (Network Access Control), służącego do monitorowania sieci lokalnych w celu uwidocznienia pracujących w nich urządzeń oraz wykrywania nowych urządzeń pojawiających się w sieci, w czasie rzeczywistym. Rozwiązanie musi raportować aktualny stan każdego urządzenia, z uwzględnieniem takich atrybutów, jak adres MAC, adres IP, nazwa hosta, system operacyjny, itp., pozyskując te informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery	

		<p>AV, WMI, itp.).</p> <p>Rozwiązanie ma za zadanie zapewnić, aby tylko urządzenia, których aktualny stan spełnia zdefiniowaną przez administratora politykę bezpieczeństwa, mogły bez ograniczeń ze strony NAC pracować w sieci lokalnej. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenia, których aktualny stan nie spełnia danych warunków polityki bezpieczeństwa (np. nowe, po raz pierwszy pojawiające się urządzenie lub stacja robocza z wyłączonym oprogramowaniem antywirusowym). Mechanizm kwarantanny powinien umożliwiać całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym, jak również blokowanie częściowe, w zakresie definiowanym przez administratora (przez wskazanie adresów IP, z którymi urządzenie może się komunikować). Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej.</p> <p>Rozwiązanie musi posiadać funkcjonalność typu Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów.</p>	
3.	Wymagania ogólne rozwiązania NAC	<ol style="list-style-type: none"> <li>1. Ma zapewnić widoczność i monitorowanie wszystkich urządzeń pracujących w sieci lokalnej oraz powiadamiać o nowych urządzeniach pojawiających się w sieci.</li> <li>2. Musi zapewniać automatyczne blokowanie komunikacji sieciowej między nowym, niezauważalnym urządzeniem a zaufanymi, zarządzanymi urządzeniami pracującymi w sieci.</li> <li>3. Musi umożliwiać sprawdzanie statusu aktualizacji oprogramowania antywirusowego i poprawek systemowych na zarządzanych stacjach roboczych Windows i w przypadku niespełniania określonych wymagań, automatycznie ograniczać tym stacjom roboczym możliwość pracy w sieci.</li> <li>4. Musi umożliwiać odbieranie komunikatów bezpieczeństwa z innych systemów bezpieczeństwa (np. firewalla) i automatyczne blokowanie na tej podstawie wskazanych urządzeń w sieci.</li> <li>5. Musi mieć funkcję wykrywania faktu skanowania urządzeń i portów wykonywanego przez urządzenie w sieci lokalnej i automatycznie blokować takie urządzenie, aby zapobiegać potencjalnemu szerzeniu się malware.</li> <li>6. Stosowany mechanizm blokowania musi wykorzystywać protokół ARP i działać całkowicie niezależnie od innych elementów infrastruktury sieciowej.</li> <li>7. Rozwiązanie musi działać bezagentowo, bez konieczności instalowania jakichkolwiek agentów na urządzeniach w sieci oraz bez konieczności dokonywania zmian w infrastrukturze sieciowej.</li> <li>8. Rozwiązanie musi umożliwiać wysyłanie alertów do administratora za pomocą e-maila oraz SMS</li> <li>9. Rozwiązanie musi być zarządzane przez interfejs webowy, obsługiwany przeglądarką internetową</li> <li>10. <b>Wymaga się, aby rozwiązanie było dostarczone w postaci maszyny wirtualnej na platformę Vmware lub Hyper-V. System musi pozwalać na monitorowanie co najmniej 5 sieci VLAN.</b></li> <li>11. <b>Wymaga się, aby rozwiązanie było licencjonowane w modelu licencji wieczystej i dostarczone z licencją pozwalającą na monitorowanie 110 urządzeń wraz ze wsparciem technicznym na okres do końca czerwca 2026</b></li> </ol>	
4.	Wymagania szczegółowe – monitorowanie podsieci	<ol style="list-style-type: none"> <li>1. Rozwiązanie musi w czasie rzeczywistym raportować widoczność wszystkich urządzeń pracujących w monitorowanych podsieciach.</li> <li>2. Rozwiązanie musi wykrywać nowe nieznanne urządzenie, dołączające się do sieci LAN lub WLAN, w czasie nie dłuższym, niż 5 sekund oraz wysyłać powiadomienie mailowe do administratora</li> <li>3. Rozwiązanie musi wykrywać przypadki skanowania urządzeń i portów w monitorowanych podsieciach i blokować urządzenie inicjujące takie skanowanie</li> <li>4. Rozwiązanie musi posiadać funkcję pułapki sieciowej (honeypot), symulującą w każdej monitorowanej podsieci standardowe usługi sieciowe, co najmniej: ssh, telnet, ftp i smb. Rozwiązanie musi rejestrować każdą próbę zalogowania się do takiej symulowanej usługi, zapisując użytą nazwę użytkownika, hasło użytkownika i źródłowy MAC/IP.</li> <li>5. Rozwiązanie musi określać aktualny stan każdego urządzenia, pozyskując informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI,</li> </ol>	



		<p>itp.) oraz odświeżać te informacje cyklicznie. Musi być możliwość wykorzystania pozyskanych informacji do definiowania polityk bezpieczeństwa.</p> <p>6. Rozwiązanie musi chronić przed podszywaniem się pod adres MAC (MAC spoofing), umożliwiając zdefiniowanie „odcisku palca” (fingerprint) dla każdego zaufanego urządzenia. Odcisk palca musi być kombinacją co najmniej: adresu MAC, adresu IP, nazwy hosta, nazwy systemu operacyjnego, otwartych portów TCP. Jeśli przeprowadzana cyklicznie weryfikacja odcisku palca wykaze jego zmianę, urządzenie powinno zostać zablokowane.</p> <p>7. Rozwiązanie musi obsługiwać VLANy, tj. umożliwiać monitorowanie przez jeden fizyczny interfejs sieciowy wielu podsieci, zdefiniowanych jako VLANy</p>	
5.	Wymagania szczegółowe – polityka bezpieczeństwa	<p>1. Rozwiązanie musi umożliwiać definiowanie polityki bezpieczeństwa, czyli określenie przez administratora, jakie warunki musi spełniać aktualny stan urządzenia, aby uzyskało ono określony dostęp do sieci.</p> <p>2. W definiowaniu polityki bezpieczeństwa musi być możliwość wykorzystania informacji o aktualnym stanie urządzenia, pozyskanych bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.), poprzez integrację z tymi systemami.</p> <p>3. Polityka bezpieczeństwa musi umożliwiać przypisanie do urządzenia jednego z trzech trybów dostępu do sieci:</p> <ul style="list-style-type: none"> <li>a. pełny dostęp</li> <li>b. blokowanie (całkowity brak dostępu)</li> <li>c. ograniczony dostęp</li> </ul> <p>4. Zakres ograniczonego dostępu powinien być definiowany przez administratora, np. w postaci list ACL, określających, do których adresów IP i portów urządzenie ma dostęp. Musi być możliwość zdefiniowania wielu różnych zakresów ograniczonego dostępu.</p> <p>5. Rozwiązanie powinno automatycznie sprawdzać, które warunki polityki bezpieczeństwa spełnia urządzenie i na tej podstawie przypisywać do urządzenia właściwy zakres dostępu.</p> <p>6. Zakres dostępu, wynikający ze spełnienia przez urządzenie danych warunków polityki bezpieczeństwa powinien być egzekwowany przez mechanizm kwarantanny.</p> <p>7. Musi być możliwość łatwego, manualnego tworzenia białej listy adresów MAC, czyli listy urządzeń mogących bez żadnych ograniczeń ze strony NAC pracować w sieci.</p>	
6.	Wymagania szczegółowe – mechanizm kwarantanny	<p>1. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenie, aby wyegzekwować ograniczenia dostępu do sieci, wynikające z polityki bezpieczeństwa</p> <p>2. Mechanizm kwarantanny powinien umożliwiać:</p> <ul style="list-style-type: none"> <li>a. całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym,</li> <li>b. częściowe blokowanie komunikacji urządzenia z otoczeniem sieciowym, w zakresie definiowanym przez administratora przez wskazanie adresów IP i portów, z którymi urządzenie może się komunikować</li> </ul> <p>3. Mechanizm kwarantanny powinien blokować komunikację urządzenia w czasie nie dłuższym niż 5 sekund od zaistnienia warunku, powodującego nałożenie kwarantanny</p> <p>4. Dla urządzeń zaufanych, czyli w polityce bezpieczeństwa spełniających kryteria pełnego dostępu do sieci, rozwiązanie nie powinno w żaden sposób przekierowywać ani blokować komunikacji wychodzącej z tych urządzeń</p> <p>5. Kwarantanna powinna być zdejmowana z urządzenia automatycznie, gdy spełni ono kryteria polityki bezpieczeństwa, pozwalające na pełny dostęp</p> <p>6. Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej, musi być niezależny od stosowanych w sieci przełączników, zarządzalnych bądź niezarządzalnych</p> <p>7. Awaria rozwiązania nie może powodować blokady komunikacji w sieci, tj. w przypadku awarii rozwiązania wszystkie urządzenia mają mieć pełny dostęp do sieci</p> <p>8. Rozwiązanie musi umożliwiać włączenie i wyłączenie mechanizmu kwarantanny (blokowania komunikacji) w każdej monitorowanej podsieci osobno</p>	
7.	Wymagania szczegółowe – integracja z systemami zewnętrznymi	<p>1. Rozwiązanie musi umieć sprawdzić, czy urządzenia z systemem Windows są dołączone do domeny AD</p> <p>2. Rozwiązanie powinno umożliwiać sprawdzanie statusu oprogramowania antywirusowego, poprawek systemowych i firewalla bezpośrednio na zarządzanych stacjach roboczych Windows w domenie AD, w sposób bezagentowy, przy użyciu WMI.</p>	



		<p>3. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym poprawkami Windows i sprawdzanie statusu zainstalowanych poprawek na zarządzanych urządzeniach z systemem Windows. Wymagana jest możliwość integracji co najmniej z systemami: Microsoft WSUS.</p> <p>4. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym agentami antywirusowymi i sprawdzanie statusu agentów AV zainstalowanych na zarządzanych urządzeniach (co najmniej, czy agent jest zainstalowany, aktywny i ma aktualne sygnatury wirusów). Wymagana jest możliwość integracji co najmniej z systemami: Bitdefender, Carbon Black, CrowdStrike, Cybereason, Eset, FireEye, McAfee, SentinelOne, Sophos, Symantec, TrendMicro, Webroot.</p> <p>5. Rozwiązanie musi umożliwiać wykorzystanie pozyskanych informacji, wymienionych w poprzedzających punktach 1-4, do definiowania polityki bezpieczeństwa.</p> <p>6. Rozwiązanie musi umieć odbierać alerty przysyłane za pomocą e-mail lub syslog z innych urządzeń bezpieczeństwa (np. firewalle) i na podstawie zawartych w nich informacji blokować wskazane podejrzone urządzenie</p>	
8.	Wymagania szczegółowe – rejestracja urządzeń zewnętrznych: pracowników, gości i konsultantów (Captive Portal)	<p>1. Rozwiązanie musi posiadać wbudowaną funkcję Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów. NAC musi przekierowywać ruch HTTP/S od nieznanych urządzeń do tego portalu.</p> <p>2. Captive Portal musi umożliwiać pracownikom rejestrowanie urządzeń prywatnych (BYOD) i wnioskowanie o dostęp do sieci w ograniczonym zakresie, zdefiniowanym przez administratora.</p> <p>3. Przy rejestracji przez pracowników ich prywatnych urządzeń, Captive Portal powinien umożliwiać użycie ich kont Active Directory</p> <p>4. Powinna istnieć możliwość ograniczenia ilości i rodzaju rejestrowanych przez pracownika prywatnych urządzeń</p> <p>5. Powinna być możliwość przypisania ograniczonego dostępu dla zarejestrowanych urządzeń prywatnych</p> <p>6. Captive Portal musi umożliwiać osobom niebędącym pracownikami (gościom lub konsultantom) wnioskowanie o ograniczony dostęp do sieci</p> <p>7. W przypadku rejestracji urządzeń gości powinna być możliwość rejestracji samodzielnie przez gościa oraz przez uprawnionego pracownika firmy</p> <p>8. Zarejestrowane urządzenia gości powinny automatycznie tracić przydzielony dostęp po upływie zdefiniowanego czasu</p> <p>9. Powinna istnieć możliwość ograniczenia ilości urządzeń rejestrowanych przez gościa</p> <p>10. Dla zarejestrowanych urządzeń gości powinna być możliwość ograniczenia, w jakich przedziałach czasu i z jakich podsieci będą one miały dostęp do sieci</p> <p>11. Dla urządzeń gości powinna być możliwość przypisania dostępu ograniczonego tylko do dostępu do internetu</p> <p>12. Dla urządzeń konsultantów powinna być możliwość przypisania dostępu ograniczonego do wybranych zasobów lokalnych</p> <p>13. Rozwiązanie musi umożliwiać zatwierdzenie dostępu dla zarejestrowanego urządzenia gościa i konsultanta drogą mailową. Osoba zatwierdzająca powinna otrzymać z systemu e-mail z wnioskiem o dostęp i udzielić go, odpowiadając na maila lub klikając przygotowany link w treści maila.</p> <p>14. Rozwiązanie musi przechowywać historyczne raporty dostępu do sieci użytkowników typu gość i konsultant</p> <p>15. Wygląd Captive Portal musi być edytowalny w zakresie co najmniej zmiany firmowego logo i kolorów oraz informacji, jakie we wniosku rejestracyjnym musi podać gość lub konsultant</p>	
9.	Pozostałe wymagania	<p>1. Rozwiązanie powinno oferować uwierzytelnianie administratora za pomocą dodatkowego faktora, oprócz hasła (2FA).</p> <p>2. Rozwiązanie powinno oferować możliwość zainstalowania opcjonalnego agenta na zarządzanych stacjach roboczych (wymagane wsparcie dla Windows, Linux i MacOS), który przesyła do serwera zarządzającego NAC szczegółowe informacje na temat stacji roboczej, umożliwiając definiowanie na bazie tych informacji precyzyjnych polityk bezpieczeństwa.</p> <p>3. Rozwiązanie nie powinno pogarszać wydajności pracy przełączników i routerów, nie może wymagać współpracy z przełącznikami przez port mirroring czy port spanning.</p>	

		4. Rozwiązanie nie powinno pogarszać wydajność łącz WAN 5. Rozwiązanie nie powinno pogarszać wydajności pracy monitorowanych urządzeń w sieci	
10.	Usługi	Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego, w wymienionym poniżej zakresie, przeprowadzoną przez wykwalifikowanego inżyniera, certyfikowanego przez producenta rozwiązania w siedzibie Zamawiającego: - instalacja i konfiguracja rozwiązania w maszynie wirtualnej na platformie Zamawiającego - szkolenie dla administratora rozwiązania - wsparcie w języku polskim w trybie 8x5 w dni robocze - kwartalny przegląd konfiguracji rozwiązania Wymaga się, aby dostawca przedstawił: - <b>oświadczenie Producenta lub Autoryzowanego Dystrybutora Producenta o posiadaniu przez dostawcę kwalifikacji technicznych, niezbędnych do wykonania wdrożenia oferowanego rozwiązania i szkolenia</b> - <b>osobowy certyfikat inżynierski pracownika, która będzie wykonywał wdrożenie,</b>	
11.	Wsparcie	Wymaga się, aby dostawca zaoferował usługę zdalnego wsparcia w zakresie reagowania na raportowane przez NAC zdarzenia, przez okres minimum do końca czerwca 2026 - w trybie ciągłym 24/7, z czasem reakcji 4 godziny, w zakresie: - alertów wysyłanych przez NAC - bieżąca analiza raportowanych zdarzeń pod kątem istniejącego zagrożenia bezpieczeństwa sieci - merytoryczne wsparcie w procesie reagowania na raportowane przez NAC zagrożenia	

#### 4 OPROGRAMOWANIE DO ARCHIWIZACJI I KATEGORYZACJI LOGÓW.

L.P.	Parametr	Wymagania minimalne	
1.	Dane producenta	Producent oferowanego rozwiązania	
2.	Charakterystyka rozwiązania	<ol style="list-style-type: none"> <li>Rozwiązanie musi odbierać wiadomości Syslog</li> <li>Rozwiązanie musi odbierać wiadomości Trap SNMP w wersji v1, v2, v3</li> <li>Rozwiązanie musi nasłuchiwać Windows Event Log</li> <li>Rozwiązanie musi posiadać graficzny interfejs użytkownika w przeglądarce internetowej</li> <li>Rozwiązanie musi mieć możliwość powiadamiania użytkowników drogą emailową na bazie otrzymanych zdarzeń</li> <li>Rozwiązanie musi mieć możliwość uruchamiania zewnętrznych skryptów</li> <li>Rozwiązanie musi mieć możliwość przesyłania dalej zebranych wiadomości do innych systemów w formatach Syslog oraz Trap SNMP w wersji v1, v2, v3</li> <li>Rozwiązanie musi mieć możliwość eksportu zdarzeń do formatu .csv</li> <li>Rozwiązanie powinno umożliwiać zarządzanie politykami retencji danych zdarzeń</li> <li>Rozwiązanie musi wspierać standard IPv4 i IPv6</li> <li>Rozwiązanie musi wspierać przesył danych na poziomie powyżej 2 000 000 zdarzeń na godzinę</li> <li>Rozwiązanie musi być licencjonowane w sposób nieograniczający ilości podłączonych urządzeń przesyłających informacje</li> <li>Rozwiązanie powinno integrować się ze Splunk</li> <li>Rozwiązanie powinno integrować się z rozwiązaniami typu SIEM</li> <li>Rozwiązanie musi mieć możliwość instalacji na systemach Microsoft Windows Server 2019, 2022, 2025 oraz Microsoft Windows 10, 11.</li> </ol>	
3.	Licencjonowanie	Licencja wieczysta na oprogramowanie, wsparcie techniczne przez okres minimum do końca czerwca 2026	
4.	Usługi	Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego, : - instalacja i konfiguracja rozwiązania na platformie Zamawiającego - szkolenie dla administratora rozwiązania - wsparcie w języku polskim w trybie 8x5 w dni robocze	

## 5 OPROGRAMOWANIE DO INWENTARYZACJI I OCHRONY PRZED WYCIEKIEM DLP - 25 LICENCJI.

LP	Parametr	Wymagania minimalne
	Dane producenta	Przedmiotem zamówienia jest dostawa licencji wieczystej i wdrożenie oprogramowania do zarządzania bezpieczeństwem IT umożliwiającego szereg funkcji podnoszących cyberbezpieczeństwo
	Architektura / budowa	<ol style="list-style-type: none"> <li>System musi umożliwić i stabilną obsługę co najmniej 25 Klientów jednocześnie.</li> <li>Architektura / budowa: <ol style="list-style-type: none"> <li>Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przysyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.</li> <li>Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).</li> <li>Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.</li> <li>Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.</li> </ol> </li> <li>Konfiguracja Architektury: <ol style="list-style-type: none"> <li>Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.</li> <li>System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.</li> </ol> </li> </ol>
	Wymagania systemowe	<ol style="list-style-type: none"> <li>Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera).</li> <li>Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2016/2019/2022/2025 Windows 7/8/8.1/10/11, Linux</li> <li>Wsparcie poniższych przeglądarek internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera, Chrome, FireFox</li> <li>Serwer musi działać na systemach 64 bitowych: Windows Server 2019/2022/2025, Windows 7/8/8.1/10/11.</li> <li>Baza danych musi działać na silniku bezpłatnym System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare i innych.</li> </ol>
	Interfejs	<ol style="list-style-type: none"> <li>System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory,</li> <li>System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL</li> <li>System zapewnia integrację z modelem LLM.</li> </ol>
	Funkcjonalności systemu zarządzania infrastrukturą IT	<ol style="list-style-type: none"> <li>System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkownika.</li> <li>Konsola administracyjna musi być w języku polskim i oferować interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie).</li> <li>W konsoli powinna istnieć funkcja filtrowania danych</li> <li>Konsola musi umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.</li> <li>Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników.</li> <li>Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników.</li> <li>System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów</li> </ol>



		<p>licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania.</p> <p>8. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office.</p> <p>9. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich połączeń.</p> <p>10. System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.</p> <p>11. System musi umożliwiać inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.</p> <p><b>Ochrona danych (DLP)</b></p> <p>12. System musi monitorować i zapobiegać wyciekom danych (DLP) poprzez bieżące (w czasie rzeczywistym) monitorowanie działań użytkowników wg ściśle zdefiniowanych polityk bezpieczeństwa oraz reguł ich opisujących.</p> <p>13. System musi zapewniać automatyczne uruchamianie ochrony zasobów w czasie rzeczywistym zgodnie ze zdefiniowanymi politykami.</p> <p>14. System musi zapewniać ciągłą ochronę danych niezależnie od położenia komputera (w sieci lokalnej, sieci VPN, poza siecią).</p> <p>15. System musi mieć możliwość konfiguracji i instalacji dowolnej ilości reguł dla dowolnych polityk DLP.</p> <p>16. System musi mieć możliwość czasowej dezaktywacji danej reguły bez jej usuwania i utraty konfiguracji.</p> <p>17. System musi w pełni wspierać następujące polityki ochrony danych: Zdefiniowanie schematu, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione. Wyświetlanie komunikatu na komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne z poziomu konsoli administracyjnej z wykorzystaniem edytora (możliwość utworzenia tabeli, dołączenia obrazu, wstawienia linku).</p> <p>18. System musi umożliwiać monitorowanie danych przesyłanych za pomocą poczty e-mail oraz blokowanie przesyłania plików określonych typów. (E-MAIL)</p> <p>19. System musi monitorować dane przesyłane do chmury oraz blokować synchronizację plików określonych typów z wybraną chmurą.</p> <p>20. System musi umożliwiać monitorowanie i blokowanie operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach.</p> <p>21. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami.</p> <p>22. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie.</p>	
--	--	--	--

	<p>23. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.</p> <p>24. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.</p> <p>25. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.</p> <p>26. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.</p> <p>27. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.</p> <p>28. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie.</p> <p>29. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.</p> <p>30. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikiem a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania.</p> <p>31. System musi posiadać możliwość eksportu / importu treści.</p> <p>32. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku. System powinien pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.</p> <p>33. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron do klasyfikacji i kontroli treści.</p> <p>34. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.</p> <p>35. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.</p> <p>36. System musi umożliwiać monitorowanie komunikatów Syslog.</p> <p>37. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.</p> <p>38. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami.</p> <p>39. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.</p> <p>40. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie</p>	
--	---	--



## Załącznik Nr 1

		<p>zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.</p> <p>41. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostępnienia w panelu pracownika.</p> <p>42. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.</p> <p>43. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki.</p> <p>44. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co predefiniowane powiadomienia oraz możliwość ich personalizacji.</p> <p>45. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymagac silnych haseł, obsługa wieloskładnikowego uwierzytelniania i posiadać mechanizmy szyfrowania danych.</p> <p>46. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizację danych i filtrami do zarządzania informacjami.</p> <p>47. System musi zapewniać kompleksowe wsparcie użytkowników poprzez helpdesk, interfejs do zgłaszania i zarządzania problemami, możliwość edycji i nadawania priorytetów zgłoszeniom oraz konfigurację powiadomień odpowiednich.</p>	
	<b>Wsparcie i pomoc</b>	<p>1. Pomoc techniczna musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.</p> <p>2. Zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.</p> <p>3. Czas trwania usługi SLA wynosi od dnia zakupu lecz nie może przekroczyć terminu 30 czerwca 2026</p>	
	<b>Wdrożenie</b>	<p>1. Komunikacja musi odbywać się w języku polskim,</p> <p>2. Wdrożenie obejmuje pełną konfigurację wszystkich modułów niezbędnych do uruchomienia systemu</p> <p>3. Wdrożenie zakończone jest szkoleniem z obsługi oprogramowania</p>	

## 6 SERWER NAS - 2 sztuki

L.p	Parametr	Charakterystyka (wymagania minimalne)	
1.	<b>Przeznaczenie</b>	Urządzenie do przechowywania danych – system NAS	
2.	Procesor	Wielordzeniowy procesor osiągający wynik minimum 4,5 tys. punktów w teście PassMark.	
3.	Obudowa	Typu rack o wysokości maksymalnie 2U z zestawem szyn przesuwanych umożliwiających montaż w szafie rack.	
4.	Pamięć RAM	Minimum 16GB DDR4 ECC tego samego producenta co serwer.	
5.	Interfejsy sieciowe	Minimum 4 porty 1GbE RJ-45. Obsługa agregacji łączy.	
6.	Ilość obsługiwanych dysków	Minimum 8 dysków o maksymalnej pojemności nie mniejszej niż 18TB każdy, po podłączeniu modułów rozszerzających minimum 12 dysków.	



7.	Zainstalowane dyski	8 dysków o pojemności 12 TB każdy zgodnych z listą kompatybilności oferowanego rozwiązania oraz charakteryzujących się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM, - gwarancja: minimum 24 miesiące, - MTBF: minimum 1 200 000 h, - możliwość aktualizacji oprogramowania dysków bezpośrednio z interfejsu systemu operacyjnego serwera NAS.	
8.	Gniazda rozszerzeń	Minimum 1 slot PCIe Gen3	
9.	Wskaźniki LED	Status, dyski, zasilanie, LAN	
10.	Obsługa RAID	RAID 0, 1, 5, 6, 10. Obsługa dysków zapasowych typu hot spare.	
11.	Funkcje RAID	Możliwość zwiększania pojemności poprzez wymianę dysków na większe. Migracja poziomu RAID w trybie online dla minimum RAID 1 i RAID 5.	
12.	Szyfrowanie	Możliwość szyfrowania wybranych udziałów sieciowych.	
13.	Protokoły	SMB, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP	
14.	Usługi	1. Serwer VPN, Serwer pocztowy, Stacja monitoringu, Windows ACL, Integracja z Windows Active Directory, Firewall, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Usługa DDNS, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki, możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów. 2. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 7 lub nowszym według harmonogramu z centralnej konsoli zarządzania dostępnej lokalnie oraz zdalnie, z możliwością przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Bez ograniczenia liczby podłączanych komputerów do systemu kopii zapasowej. 3. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klastr obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora.	
15.	Zarządzanie dyskami	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów,	
16.	System plików	Dyski wewnętrzne: BTRFS, EXT4 Dyski zewnętrzne: FAT, NTFS, EXT3, EXT4, HFS+.	
17.	Język GUI	Polski	
18.	Certyfikaty	CE,	
19.	Szyfrowanie	Mechanizm szyfrowania sprzętowego.	
20.	Zasilanie	Pojedynczy zasilacz o mocy maksymalnie 350W.	
21.	Opcje software'owe	1. zarządzanie NAS poprzez minimum przeglądarkę internetową, GUI oparte o HTML5; 2. NAS musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania NAS; 3. NAS musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową; 4. NAS musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów NAS, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – nie jest wymagane dostarczenie licencji dla tej funkcjonalności; 5. Serwer plików, Serwer FTP, WebDav, Serwer WEB, Serwer kopii zapasowych, Serwer Monitoringu,	
22.	Konfiguracja, zarządzanie	1. komunikacja z wbudowanym oprogramowaniem zarządzającym NAS musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW jak również w trybie tekstowym. 2. musi być możliwe zdalne zarządzanie NAS z wykorzystaniem standardowej przeglądarki internetowej (np. Edge, Opera, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora	
23.	Gwarancja i serwis	1. 2 lata gwarancji producenta NAS w trybie onsite z gwarantowanym czasem skutecznej naprawy najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw.	

		tryb Next Business Day); 2. Gwarancja producenta na dyski: 2 lat 3. uszkodzone dyski zawierające dane pozostają własnością Zamawiającego i nie będą zwracane do serwisu producenta NAS, w ich miejsce w ramach 2-letniego okresu gwarancji zostaną dostarczone nowe; 4. serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego,	
24.	Jakość produktu i sposobu jego wykonania	Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany NAS spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta NAS lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych.	

## 7 PRZELĄCZNIKI ZARZĄDZALNE – 3 szt

L.P	Parametr	Charakterystyka (wymagania minimalne)	
1.	<b>CECHY ZARZĄDZANIA</b>		
2.	Typ przełącznika	Zarządzany	
3.	Przełącznik wielowarstwowy	L2/L3	
4.	Obsługa jakości serwisu (QoS)	Tak	
5.	Zarządzany w chmurze	Tak	
6.	Zarządzanie przez stronę www	Tak	
7.	Inspekcja ARP	Tak	
8.	Konfigurowanie ustawień lokalizacji (CLI)	Tak	
9.	Obsługa MIB	Tak	
10.	<b>OCHRONA</b>		
11.	Funkcje DHCP	DHCP relay, DHCP server, DHCPv6 client	
12.	Lista kontrolna dostępu (ACL)	Tak	
13.	Zasady Listy Kontroli Dostępu (ACL)	1024	
14.	IGMP snooping	Tak	
15.	Ochrona hasłem	Tak	
16.	obsługuje SSH/SSL	Tak	
17.	Zabezpieczenie DoS	Tak	
18.	Filtrowanie adresów MAC	Tak	
19.	Szyfrowanie / bezpieczeństwo	HTTPS, SSH, SSL/TLS	
20.	<b>PORTY I INTERFEJSY</b>		
21.	Podstawowe przełączanie RJ-45 Liczba portów Ethernet	48	

## Załącznik Nr 1

22.	Podstawowe przełączania Ethernet RJ- 45 porty typ	Gigabit Ethernet (10/100/1000)	
23.	Ilość slotów Modułu SFP+	4	
24.	Liczba portów konsoli	RJ-45, USB typ C	
25.	Wydajność	Przepustowość przełącznika nie może być mniejsza niż 176Gb/s. Szybkość przełączania ramek wewnątrz przełącznika nie może być mniejsza niż 130,9Mp/s.	
26.	<b>SIEĆ</b>		
27.	Standardy komunikacyjne	EEE 802.1Q, IEEE 802.1ab, IEEE 802.1ad, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ad, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z	
28.	Obsługa 10G	Tak	
29.	Dublowanie portów	Tak	
30.	Protokół drzewa rozpinającego	Tak	
31.	Blokowanie head-of-line (HOL)	Tak	
32.	Prędkość transferu danych przez Ethernet LAN	10,100,1000 Mbit/s	
33.	Kontrola wzrostu natężenia ruchu	Tak	
34.	Automatyczne MDI/MDI- X	Tak	
35.	Podpora kontroli przepływu	Tak	
36.	Agregator połączenia	Tak	
37.	Obsługa sieci VLAN	Tak	
38.	Liczba VLANs	4094	
39.	<b>PRZESYŁANIE DANYCH</b>		
40.	Wielkość tabeli adresów	16000 wejścia	
41.	Zgodny z Jumbo Frames	Tak	
42.	Rozszerzenie Jumbo Frames	9000	
43.	<b>FUNKCJE MULTICAST</b>		
44.	Obsługa Multicast	Tak	
45.	<b>PROTOKOŁY</b>		
46.	Protokoły zarządzające	CLI, SNMP, Telnet, SSH, SSH-2, DHCP, SCP, HTTPS, HTTP, ICMP, TFTP, Syslog, SNMP 2c, SNMP 3, RMON, RADIUS	
47.	<b>KONSTRUKCJA</b>		
48.	Możliwości montowania w stelażu	Tak	
49.	Przycisk reset	Tak	
50.	Diody LED	Tak	
51.	<b>WYDAJNOŚĆ</b>		
52.	Procesor wbudowany wielordzeniowy	Tak	
53.	Taktowanie procesora	1.4 GHz	
54.	Pojemność pamięci flash	1 GB	
55.	Pojemność pamięci RAM	1 GB	



## Załącznik Nr 1

56.	Aktualizacje oprogramowania urządzenia	Tak	
57.	<b>MOC</b>		
58.	Zasilacz dołączony	Tak	
59.	<b>GWARANCJA</b>		
60.	Gwarancja	Dożywotnia producenta (min. do 60 miesięcy od wycofania z produkcji/sprzedaży przez producenta)	

## 8 UPS CENTRALNY – 1 KPL.

L.P.	Parametr	Wymagania minimalne	
1.	Moc pozorna	min. 6000VA	
2.	Moc rzeczywista	min. 6000W	
3.	Technologia	on-line (VFI), podwójna konwersja	
4.	Sprawność max (dla VFI)	> 92 %	
5.	Typ obudowy	rack/tower	
6.	Poziom hałasu	< 55dB	
7.	<b>parametry wejściowe</b>		
8.	Napięcie wejściowe	208 V AC / 220 V AC / 230 V AC / 240 V AC	
9.	Zakres napięcia wejściowego	80-300 V AC	
10.	Zakres częstotliwości wejściowej	45~55 / 54~66 Hz	
11.	<b>parametry wyjściowe</b>		
12.	Zakres napięcia wyjściowego	208 V AC / 220 V AC / 230 V AC / 240 V AC	
13.	Częstotliwość napięcia wyjściowego	50 / 60 Hz (+/- 0,5%)	
14.	Kształt napięcia wyjściowego	sinusoidalny	
15.	Czas przełączania sieć – UPS	0ms	
16.	Współczynnik odkształceń THDv	<2% liniowe obciążenie; < 5% @ nieliniowe obciążenie	
17.	Przebieżalność w trybie sieciowym	minimum 105-110% = 10 min, 110-130% = 1 min, >130% = przejście w bypass po 3 sek.	
18.	Przebieżalność w trybie bateryjnym	minimum 105-110% = 10 min, 110-130% = 1 min, >130% = przejście w bypass po 3 sek.	
19.	Baterie wewnętrzne w UPS lub w zewnętrznym module bateryjnym	minimum 12V 9Ah; szczelne, bezobsługowe	
20.	Czas podtrzymania (dla 50 % Pmax) - przy zastosowaniu baterii wew. lub z 1 zewnętrznym modulem bateryjnym	minimum 9 min	
21.	Możliwość podłączenie zewnętrznych modułów bateryjnych	wymagane	
22.	Możliwość włączenia testu baterii	wymagane	
<b>pozostałe</b>			
23.	Wejście zasilania	listwa zaciskowa / terminal śrubowy	
24.	Ilość i typ gniazd wyjściowych	listwa zaciskowa / terminal śrubowy oraz 4x IEC320 C19 + 2x IEC320 C13	
25.	Sygnalizacja	Wyświetlacz LCD, akustyczna	
26.	Informacje do odczytania z poziomu LCD	minimum napięcie wejściowe i wyjściowe, częstotliwość wejściowa i wyjściowa, obciążenie w procentach oraz obciążenie w watach lub kilowatach, praca w trybie sieciowym, bateryjnym, ECO, BYPASS, procentowa pojemność baterii, napięcie baterii, błąd baterii, niski poziom baterii, przeciążenie, pozostały czas pracy bateryjnej w minutach	

## Załącznik Nr 1

27.	Test baterii	wymagana możliwość ustawienia automatycznego testu baterii w zakresie 1 do 45 dni	
28.	Możliwość pracy w trybie konwertera częstotliwości	wymagane	
29.	Automatyczne ładowanie po powrocie zasilania	wymagane	
30.	Automatyczne uruchomienie po powrocie zasilania	wymagane	
31.	Interfejs komunikacyjny	RS232, USB, SNMP	
32.	Funkcja ROO - zdalne włączenie / wyłączenie zasilania	wymagane	
33.	Wymagania odnośnie interfejsu sieciowego	obsługa protokołu SNMP v1 i v3, HTTP/HTTPS, SSH	
		wsparcie dla IPv4 oraz IPv6	
		możliwość ustawienia hasła o długości 8 znaków	
		możliwość wyłączenia wybranych kanałów komunikacyjnych z urządzeniem	
		wsparcie dla LDAP lub RADIUS	
		dostęp do bazy danych MIB zgodnej z RFC 1628	
34.	Złącze EPO	wymagane	
35.	Wsporniki do montażu w szafie RACK	wymagane	
36.	Zewnętrzny bypass serwisowy w wersji rack lub naściennej, tego samego producenta co oferowany UPS	wymagany	
37.	Waga UPS	do 15kg	
38.	Wymiary UPS - wersja RACK	nie większe niż: wysokość 3U; głębokość 700 mm	
39.	Waga Moduł Baterijny - jeżeli występuje	do 70 kg	
40.	Wymiary Moduł Baterijny - wersja RACK - jeżeli występuje	nie większe niż: wysokość 3U; głębokość 700 mm	
41.	Gwarancja	minimum 24 miesiące na elektronikę i 24 miesiące na baterie	
42.	Serwis	autoryzowany serwis producenta zlokalizowany w Polsce.	
		naprawa w maksymalnie 5 dni roboczych	
		serwis realizowany w systemie door to door	
43.	Oprogramowanie	wsparcie dla systemów: Windows, Linux	
		wymagane wsparcie producenta w języku polskim (telefoniczne oraz mailowe)	
44.	Oświadczenia / dokumenty	oświadczenie producenta lub wyłącznego dystrybutora o spełnieniu minimalnych wymaganych parametrów specyfikacji	
		dla gwarancja standardowej lub rozszerzonej wymagane jest by realizowana była wyłącznie przez autoryzowany serwis producenta - należy przedstawić odpowiednie oświadczenie producenta lub wyłącznego dystrybutora	
		certyfiat lub oświadczenie producenta lub wyłącznego dystrybutora o posiadaniu przez oferenta statusu Autoryzowanego Partnera - mającego wiedzę w zakresie doboru i sprzedaży zasilania gwarantowanego (UPS) jeżeli oferent nie jest producentem sprzętu. deklaracja zgodności CE	

45.	Dodatkowe usługi	Podłączenie do przygotowanej instalacji elektrycznej (wyprowadzonych przez zamawiającego kabli). Podłączenie wyłącznie przez Autoryzowany Serwis Producenta uwzględniające podłączenie UPS, podłączenie modułu baterijnego (jeżeli występuje), podłączenie bypassu do wejścia zasilania oraz do UPSa (jeżeli występuje), montaż w szafie rack, pierwsze uruchomienie, szkolenie z obsługi
-----	------------------	---

## 9 ZASADA RÓWNOWAŻNOŚCI ROZWIĄZAŃ I NEUTRALNOŚCI TECHNOLOGICZNEJ.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań lub też stosowane jest w celu wskazania aktualnie użytkowanego środowiska Zamawiającego, z którym rozwiązanie równoważne powinno być kompatybilne.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełniają zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.
5. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznaczących różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.
9. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia poprawności przeprowadzonych testów może wezwać Wykonawcę do przedstawienia wskazanego przez Zamawiającego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowania overclockingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
10. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający dopuszcza równoważne im testy wydajnościowe umożliwiające potwierdzenie zakładanych poziomów wydajności. W przypadku użycia przez Wykonawcę równoważnych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia równoważności przeprowadzonych testów Wykonawca może zostać wezwany do dostarczenia Zamawiającemu wskazanego przez Zamawiającego oprogramowania testującego i równoważnego do niego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowania overclockingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).



Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.

11. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.
12. Za równoważną do normy ISO 9001 Zamawiający uzna normę, która dotyczy zarządzania jakością ustanawiając wymagania dla systemów zarządzania jakością w organizacjach w minimum następującym zakresie:
  - 1) Skupienie na użytkowniku – Podstawowym celem systemu zarządzania jakością jest zwiększenie satysfakcji użytkownika poprzez spełnianie jego wymagania oraz oczekiwania. Organizacja powinna monitorować potrzeby użytkowników i dostarczać produkty lub usługi, które je zaspokajają.
  - 2) Przywództwo – Wspieranie kierownictwa w zapewnianiu odpowiednich zasobów i wsparcia w procesach zarządzania jakością. Przywódcy powinni tworzyć środowisko, które wspiera zaangażowanie pracowników w poprawę jakości.
  - 3) Zaangażowanie ludzi – Organizacja powinna zapewnić, aby wszyscy pracownicy byli zaangażowani w realizację celów jakościowych. Kluczowym elementem jest angażowanie personelu w procesy poprawy jakości i podejmowanie działań na rzecz doskonalenia.
  - 4) Podejście procesowe – Norma podkreśla, że organizacja powinna zarządzać swoimi procesami w sposób spójny i skuteczny, traktując je jako powiązane ze sobą elementy systemu zarządzania jakością, które wspólnie prowadzą do osiągnięcia celów organizacji.
  - 5) Podejście systemowe do zarządzania – Organizacja powinna traktować system zarządzania jakością jako całość, złożoną z wzajemnie powiązanych elementów (np. procesów, zasobów, technologii), które muszą działać w harmonii, aby osiągnąć cele jakościowe.
  - 6) Ciągłe doskonalenie – dążenie do ciągłego doskonalenia procesów w organizacji. Ciągłe doskonalenie jest kluczowym elementem skutecznego zarządzania jakością i poprawy wyników.
  - 7) Podejście do podejmowania decyzji oparte na faktach – w procesie podejmowania decyzji organizacja powinna opierać się na danych i analizach, a nie na przypuszczeniach czy intuicji. Podejście to pozwala na bardziej precyzyjne i obiektywne decyzje.
  - 8) Relacje z dostawcami na zasadzie wzajemnych korzyści – tworzenie partnerskich relacji z dostawcami, które będą korzystne dla obu stron. Współpraca z dostawcami powinna być oparta na zaufaniu i dążeniu do wspólnych celów jakościowych.
  - 9) Zarządzanie ryzykiem – norma wymaga, aby organizacje identyfikowały, oceniały i zarządzały ryzykiem związanym z procesami oraz ich wpływem na zdolność organizacji do dostarczania produktów i usług o wymaganej jakości.
  - 10) Dokumentowanie systemu zarządzania jakością – Norma określa wymagania dotyczące dokumentowania systemu zarządzania jakością, w tym tworzenia polityki jakości, procedur, instrukcji roboczych oraz zapisów, które umożliwiają monitorowanie i weryfikację skuteczności systemu.
13. Za równoważną do normy ISO 50001 Zamawiający uzna normę, która dotyczy zarządzania energią w organizacjach w minimum następującym zakresie:
  - 1) Skupienie na poprawie efektywności energetycznej – Celem normy jest poprawa efektywności wykorzystania energii poprzez identyfikację obszarów, w których możliwe są oszczędności i usprawnienia w zarządzaniu energią.
  - 2) Zarządzanie cyklem życia energii – uwzględnia cały cykl życia energii, od planowania, poprzez wykorzystanie, aż po monitorowanie, ocenę i doskonalenie działań mających na celu zmniejszenie zużycia energii.
  - 3) Zintegrowane podejście z innymi systemami zarządzania – Norma jest zaprojektowana w sposób zgodny z innymi międzynarodowymi normami, co umożliwia integrację systemów zarządzania w organizacji.
  - 4) Podejście oparte na cyklu PDCA (Plan-Do-Check-Act) – opiera się na cyklu PDCA, który wspiera organizacje w procesie ciągłego doskonalenia zarządzania energią poprzez planowanie, wdrażanie, monitorowanie i działania korygujące.
  - 5) Zaangażowanie kierownictwa – Norma wymaga, aby najwyższe kierownictwo organizacji angażowało się w proces zarządzania energią, podejmując decyzje, dostarczając zasoby oraz ustalając cele i polityki energetyczne.
  - 6) Ustalenie polityki energetycznej – norma zachęca organizacje do opracowania polityki energetycznej, która definiuje kierunki działań, cele efektywności energetycznej oraz zobowiązania do ciągłego doskonalenia.
  - 7) Identyfikacja i ocena aspektów energetycznych – Norma wymaga przeprowadzenia analizy aspektów energetycznych, które mają istotny wpływ na zużycie energii i środowisko, oraz wdrożenia działań na rzecz ich poprawy.

## Załącznik Nr 1

- 8) Monitorowanie, pomiar i analiza – nakłada obowiązek monitorowania i mierzenia zużycia energii oraz wydajności energetycznej organizacji. Organizacja powinna także stosować odpowiednie narzędzia do analizy wyników, identyfikacji możliwości poprawy oraz podejmowania działań korygujących.
  - 9) Zarządzanie ryzykiem i szansami – Norma podkreśla znaczenie identyfikacji ryzyk i szans związanych z zarządzaniem energią, a także działań na rzecz minimalizowania ryzyka i maksymalizowania możliwości poprawy efektywności energetycznej.
  - 10) Ciężar działań edukacyjnych i szkoleń – Norma wskazuje na konieczność zapewnienia odpowiedniego poziomu wiedzy i umiejętności w zakresie zarządzania energią dla wszystkich pracowników organizacji. Szkolenia i podnoszenie świadomości energetycznej są kluczowe dla skutecznego wdrażania polityki energetycznej.
14. Za równoważną do normy ISO 14001 Zamawiający uzna normę, która dotyczy systemów zarządzania środowiskowego w minimum następującym zakresie:
- 1) Zarządzanie środowiskowe oparte na cyklu PDCA (Plan-Do-Check-Act) – norma opiera się na cyklu PDCA, który wspiera organizację w systematycznym zarządzaniu i doskonaleniu ich działań na rzecz ochrony środowiska. Proces obejmuje planowanie, wdrażanie, monitorowanie oraz podejmowanie działań korygujących.
  - 2) Zobowiązanie organizacji do ochrony środowiska – Norma wymaga, aby organizacja była zobowiązana do minimalizowania negatywnego wpływu na środowisko. To zobowiązanie powinno być wyrażone poprzez politykę środowiskową, która wskazuje na cele ochrony środowiska.
  - 3) Identyfikacja aspektów środowiskowych – Organizacja musi identyfikować i oceniać aspekty środowiskowe związane z jej działalnością, produktami i usługami. Ocena powinna uwzględniać wpływ na środowisko, zarówno w zakresie zużycia zasobów, jak i wytwarzania odpadów oraz emisji.
  - 4) Zgodność z przepisami prawnymi i innymi wymaganiami – norma wymaga, aby organizacja przestrzegała obowiązujących przepisów prawnych dotyczących ochrony środowiska oraz innych zobowiązań, które organizacja uzna za stosowne (np. normy branżowe).
  - 5) Cele środowiskowe i planowanie działań – Organizacja musi wyznaczać mierzalne cele środowiskowe i opracować plany działań, które pozwolą osiągnąć te cele. Cele te powinny być zgodne z polityką środowiskową i uwzględniać aspekt środowiskowy w całym cyklu życia produktów i usług.
  - 6) Zaangażowanie kierownictwa – zaangażowanie najwyższego kierownictwa w wdrażanie systemu zarządzania środowiskowego. Kierownictwo powinno zapewnić zasoby, nadzór i wspierać działania na rzecz ochrony środowiska.
  - 7) Zarządzanie ryzykiem środowiskowym – Norma podkreśla konieczność identyfikacji i oceny ryzyk środowiskowych związanych z działalnością organizacji. Organizacja powinna podejmować działania na rzecz minimalizowania ryzyka, a także wdrażać procedury zapobiegania i reagowania na sytuacje kryzysowe.
  - 8) Monitorowanie, pomiar i analiza wyników – Organizacja jest zobowiązana do monitorowania i mierzenia skuteczności swoich działań środowiskowych. Obejmuje to ocenę wpływu działań na środowisko, skuteczność realizacji celów oraz identyfikację obszarów do poprawy.
  - 9) Działania korygujące i zapobiegawcze – norma wymaga, aby organizacja wdrażała procedury podejmowania działań korygujących w przypadku niezgodności oraz działań zapobiegawczych, aby uniknąć powtarzania się problemów środowiskowych w przyszłości.
  - 10) Ciągłe doskonalenie systemu zarządzania środowiskowego – Podstawowym celem normy jest dążenie do ciągłego doskonalenia systemu zarządzania środowiskowego. Organizacja powinna regularnie przeglądać i aktualizować swoje cele, polityki i procesy, aby dostosować je do zmieniających się warunków środowiskowych oraz wymagań prawnych.
15. Za równoważną do normy ISO 27001 Zamawiający uzna normę, która określa standard zarządzania bezpieczeństwem informacji w minimum następującym zakresie: Zarządzanie ryzykiem – norma stosuje podejście oparte na zarządzaniu ryzykiem. Organizacja musi przeprowadzać ocenę ryzyka dla bezpieczeństwa informacji i podejmować odpowiednie środki w celu zarządzania tym ryzykiem.
- 1) Ochrona informacji – Norma zapewnia, że organizacja identyfikuje, ocenia i zabezpiecza informacje, w tym dane osobowe, finansowe, techniczne, i inne zasoby przed zagrożeniami.
  - 2) Ciągłość działania – norma kładzie nacisk na ciągłość działania w przypadku awarii systemów, katastrof naturalnych, ataków cybernetycznych itp. Organizacje muszą przygotować plany awaryjne i procedury odzyskiwania danych.
  - 3) Zaangażowanie kierownictwa – Norma wymaga aktywnego zaangażowania najwyższego kierownictwa w procesie zarządzania bezpieczeństwem informacji.
  - 4) Ciągłe doskonalenie – norma promuje ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji, aby dostosować go do zmieniających się zagrożeń i wymagań.
  - 5) Polityki bezpieczeństwa informacji – norma określa, że organizacja musi opracować i wdrożyć formalne polityki bezpieczeństwa informacji, które są zgodne z jej celami biznesowymi i wymaganiami regulacyjnymi.
  - 6) Szkolenia i świadomość pracowników – norma kładzie nacisk na edukację i szkolenia pracowników w zakresie bezpieczeństwa informacji. Wszyscy pracownicy muszą być świadomi swoich obowiązków w zakresie ochrony danych.
  - 7) Zarządzanie dostępem – norma wymaga, aby dostęp do informacji i zasobów organizacji był kontrolowany i ograniczony na podstawie ról i odpowiedzialności pracowników.
  - 8) Monitorowanie i przeglądy – norma określa, że organizacje muszą regularnie monitorować skuteczność wdrożonego systemu zarządzania bezpieczeństwem informacji oraz przeprowadzać audyty, które pozwolą ocenić zgodność z wymaganiami normy.
  - 9) Zgodność z przepisami prawa – norma wymaga, aby organizacje zapewniały zgodność z obowiązującymi przepisami prawnymi dotyczącymi ochrony danych osobowych, ochrony prywatności i bezpieczeństwa informacji.
16. Za równoważną do regulacji RoHS Zamawiający uzna regulację, która dotyczy stosowania substancji niebezpiecznych w sprzęcie elektrycznym i elektronicznym w minimum następującym zakresie:



## Załącznik Nr 1

- 1) Zakaz stosowania niebezpiecznych substancji – ogranicza użycie sześciu substancji niebezpiecznych w sprzęcie elektrycznym i elektronicznym: ołów (Pb), rtęć (Hg), kadm (Cd), sześciowartościowy chrom (Cr<sup>6</sup>), polibromowane bifenyle (PBB) i polibromowane etery difenylowe (PBDE).
  - 2) Zastosowanie do sprzętu elektronicznego i elektrycznego – obejmuje szeroki zakres produktów, takich jak telewizory, komputery, sprzęt AGD, zabawki, oświetlenie LED, urządzenia medyczne, sprzęt telekomunikacyjny i inne urządzenia elektroniczne.
  - 3) Zobowiązanie producentów do zgodności – Producenci i importerzy sprzętu elektrycznego i elektronicznego muszą zapewnić, że ich produkty nie zawierają zabronionych substancji powyżej dopuszczalnych poziomów.
  - 4) Oświadczenia o zgodności – Producenci są zobowiązani do dostarczania odpowiednich oświadczeń o zgodności z regulacją. Powinny one być udostępniane organom nadzoru oraz użytkownikom w razie potrzeby.
  - 5) Kontrola i nadzór rynkowy – regulacja nakłada obowiązek przeprowadzania kontroli rynkowych przez odpowiednie organy państwowe, aby upewnić się, że produkty wprowadzane na rynek UE spełniają wymogi dyrektywy.
  - 6) Ograniczenie wpływu na zdrowie i środowisko – celem regulacji jest zmniejszenie negatywnego wpływu niebezpiecznych substancji na zdrowie ludzi oraz na środowisko naturalne, szczególnie podczas recyklingu i utylizacji odpadów elektronicznych.
  - 7) Zdolność do recyklingu i odzysku – regulacja promuje projektowanie produktów w sposób, który umożliwia ich łatwiejszy recykling i utylizację. Przepisy zakładają, że zabronione substancje nie mogą występować w produktach w ilościach, które utrudniają ich odzyskiwanie.
  - 8) Zakres geograficzny – regulacja ma zastosowanie w krajach Unii Europejskiej oraz w krajach, które przyjęły odpowiednie przepisy zgodne z dyrektywą.
  - 9) Obowiązki w przypadku modyfikacji produktów – W przypadku wprowadzenia istotnych zmian w produkcie (np. zmiana jego konstrukcji), producent musi upewnić się, że nowa wersja również spełnia wymagania regulacji. Dotyczy to również produktów wprowadzanych na rynek wtórny (np. w ramach naprawy lub refabrykacji).
17. Za równoważną do regulacji CE Zamawiający uzna regulację, która spełnia wszystkie odpowiednie wymagania dotyczące zdrowia, bezpieczeństwa oraz ochrony środowiska, zgodnie z przepisami UE w minimum następującym zakresie:
- 1) Potwierdzenie zgodności z wymaganiami UE – formalne oświadczenie producenta lub importera, że dany produkt spełnia wszystkie obowiązujące przepisy unijne dotyczące zdrowia, bezpieczeństwa, ochrony środowiska i innych przepisów regulujących dany produkt.
  - 2) Oznakowanie CE – posiada system oznaczeń, który wskazuje, że produkt przeszedł ocenę zgodności i jest dopuszczony do sprzedaży w Unii Europejskiej.
  - 3) Szczegółowe informacje o producencie – dokument potwierdzający musi zawierać pełne dane producenta (lub importera), takie jak nazwa firmy, adres siedziby, a także dane kontaktowe. W przypadku importera – także informacje o tym, kto odpowiada za dany produkt w UE.
  - 4) Opis produktu – dokument potwierdzający musi zawierać szczegółowy opis produktu, który obejmuje nazwę produktu, numer referencyjny lub numer katalogowy, a także inne identyfikatory, które umożliwiają jednoznaczną identyfikację produktu.
  - 5) Odniesienia do odpowiednich norm – dokument potwierdzający wskazuje normy, dyrektywy lub przepisy unijne, z którymi produkt jest zgodny.
  - 6) Procedura oceny zgodności – dokument potwierdzający musi wskazywać, w jaki sposób ocena zgodności produktu została przeprowadzona (np. przez samodzielną ocenę producenta lub poprzez współpracę z jednostką notyfikowaną w przypadku bardziej skomplikowanych produktów).
  - 7) Data i miejsce sporządzenia deklaracji – dokument potwierdzający powinien zawierać datę sporządzenia deklaracji oraz miejsce jej podpisania, co ma znaczenie prawne i daje pewność co do okresu ważności oświadczenia.
  - 8) Podpis osoby upoważnionej – dokument potwierdzający musi być podpisana przez osobę upoważnioną w imieniu producenta lub importera, która jest odpowiedzialna za prawdziwość oświadczenia. Zwykle jest to przedstawiciel firmy, który ma uprawnienia do składania oświadczeń w imieniu organizacji.
  - 9) Wymóg dostępności dla organów nadzoru – dokument potwierdzający musi być dostępny dla odpowiednich organów nadzoru rynkowego, które mogą przeprowadzać kontrole w celu weryfikacji zgodności produktów z obowiązującymi wymaganiami.
  - 10) Zakres odpowiedzialności producenta – dokument potwierdzający musi być dokumentem, który wiąże producenta z odpowiedzialnością za zgodność produktu z wymaganiami prawnymi i normatywnymi. Jeżeli produkt nie spełnia wymagań, producent lub importer mogą być pociągnięci do odpowiedzialności za naruszenie przepisów UE.
18. Za równoważną do certyfikacji FIPS 140-2 Zamawiający uzna certyfikację, która dotyczy standardu wymagań bezpieczeństwa dla modułów kryptograficznych w minimum następującym zakresie:
- 1) Obejmuje wszystkie komponenty sprzętowe, oprogramowanie i kombinacje tych elementów, które realizują operacje kryptograficzne (np. szyfrowanie, podpisy cyfrowe, generowanie kluczy).
  - 2) Wymaga, aby moduły kryptograficzne posiadały odpowiednią ochronę przed manipulacjami fizycznymi.
  - 3) Wymaga, aby wszystkie klucze kryptograficzne były odpowiednio chronione. Obejmuje to m.in. przechowywanie, generowanie, zarządzanie i wymianę kluczy w sposób, który zapobiega ich nieautoryzowanemu ujawnieniu.
  - 4) Nakłada wymagania dotyczące bezpiecznego uruchamiania modułu kryptograficznego, w tym procedury inicjalizacji, które muszą zapewniać, że urządzenie jest w pełni zabezpieczone przed uruchomieniem jakichkolwiek operacji kryptograficznych.
  - 5) Wymaga, aby systemy kryptograficzne były testowane pod kątem zabezpieczeń kryptograficznych.
  - 6) Definiuje wymagania dotyczące implementacji standardowych algorytmów kryptograficznych.
  - 7) Wymaga, aby systemy kryptograficzne były odpowiednio utrzymywane przez cały okres ich użytkowania.



**UMOWA NR .../2026**

zawarta w dniu .....**2026 r.** w Potoku Górnym pomiędzy:  
**Gminą Potok Górny** z siedzibą w **Potok Górny 116, 23-423 Potok Górny**  
zwaną dalej „**Zamawiającym**”,

reprezentowaną w niniejszej Umowie przez:

**Pan Stanisław Dyjak** – Wójt Gminy Potok Górny  
przy kontrasygnacie Skarbnika Gminy Potok Górny – **Pani Aurelii Ćwikła**

**a**

\*gdy kontrahentem jest spółka prawa handlowego:

spółką pod firmą „...” z siedzibą w ... (wpisać tylko nazwę miasta/miejscowości),  
ul. ...., ..... (wpisać adres), wpisaną do Rejestru Przedsiębiorców Krajowego  
Rejestru Sądowego pod numerem KRS ....., NIP ....., REGON  
....., zwaną dalej „Wykonawcą”, reprezentowaną przez .....<sup>1</sup>/reprezentowaną  
przez ... działającą/-ego na podstawie pełnomocnictwa, stanowiącego załącznik do umowy<sup>2</sup>,

\*gdy kontrahentem jest osoba fizyczna prowadząca działalność gospodarczą:

Panią/Panem ....., prowadzącą/-ym działalność gospodarczą pod firmą „...” zamieszkałym w  
... (wpisać tylko nazwę miasta/miejscowości), ul. .... (wpisać adres), NIP  
....., REGON ....., , zwaną/-ym dalej „Wykonawcą”, reprezentowaną/-ym przez ...  
działającą/-ego na podstawie pełnomocnictwa, stanowiącego załącznik do umowy<sup>3</sup>,  
wspólnie zwanymi dalej „Stronami”.

Strony oświadczają, że niniejsza umowa, zwana dalej „umową”, została zawarta  
w wyniku udzielenia zamówienia publicznego w trybie podstawowym, zgodnie  
z przepisami ustawy z dnia 11 września 2019 r. (Dz. U. z 2024 r. poz. 1320 z późn. zm.) – Prawo  
zamówień publicznych.

**Oświadczenia Stron**

1. Strony oświadczają, że niniejsza umowa, zwana dalej „umową”, została zawarta w wyniku przeprowadzonego postępowania o udzielenie zamówienia publicznego w trybie podstawowym zgodnie z art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320 t. j. z późn. zm.),
2. Zamawiający i Wykonawca zobowiązują się współdziałać przy wykonaniu umowy w sprawie zamówienia publicznego w celu należytej realizacji zamówienia.

**§ 1****Przedmiot umowy**

1. Przedmiotem zamówienia jest realizacja zadania pn. „**Zakup sprzętu IT wraz z oprogramowaniem w ramach projektu Zwiększenie cyberbezpieczeństwa Gminy Potok Górny**” w zakresie **Część 1 Dostawa serwerów z oprogramowaniem**.
2. Zadanie realizowane jest w związku z realizacją projektu pn. „**Zwiększenie cyberbezpieczeństwa Gminy Potok Górny**”, współfinansowanego ze środków Unii

<sup>1</sup>

Jeżeli przy zawarciu umowy działa osoba/-y pełniąca/-e funkcję organu (członka organu) lub prokurent spółki.

<sup>2</sup>

Jeżeli przy zawarciu umowy działa pełnomocnik spółki.

<sup>3</sup>

Jeżeli przy zawarciu umowy działa pełnomocnik tej osoby.

Europejskiej i budżetu państwa w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Priorytetu II Zaawansowane usługi cyfrowe, Działania 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.01-001/23/2520/ FERC.02.02-CS.01-001/23/2024.

3. Przedmiotem Umowy jest:

- 1) Zakup serwera z oprogramowaniem typ I
- 2) Zakup serwera z oprogramowaniem typ II
- 3) Zakup i wdrożenie rozwiązania Network Access Control
- 4) Zakup oprogramowania do archiwizacji i kategoryzacji logów
- 5) Zakup oprogramowania do inwentaryzacji i ochrony przed wyciekiem DLP

4. W ramach realizacji zamówienia Wykonawca zobowiązuje się w szczególności do:

- 1) dostawy sprzętu informatycznego oraz oprogramowania określonego w SOPZ,
  - 2) instalacji, konfiguracji oraz uruchomienia dostarczonych urządzeń i systemów,
  - 3) wdrożenia systemów informatycznych zgodnie z wymaganiami określonymi w SOPZ,
  - 4) integracji dostarczonych rozwiązań z istniejącą infrastrukturą informatyczną Zamawiającego, jeżeli jest to wymagane,
  - 5) przeprowadzenia szkolenia administratorów Zamawiającego w zakresie obsługi dostarczonych systemów, jeżeli wymagane takie wynika z SOPZ,
  - 6) przekazania dokumentacji technicznej oraz powdrożeniowej dotyczącej dostarczonych urządzeń i systemów.
5. Szczegółowy zakres zamówienia określony jest w Specyfikacji Warunków Zamówienia oraz w załączonym do SWZ Szczegółowym Opisie Przedmiotu Zamówienia Załącznik nr 1 do SWZ.
6. Dostarczany przedmiot umowy musi być fabrycznie nowy, nieużywany, nieuszkodzony i nieobciążony prawami osób trzecich oraz muszą pochodzić z oficjalnego kanału dystrybucyjnego w UE.
7. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą się znajdować się na liście „end-of-sale” oraz „end-of-support” producenta, nie dopuszcza w żadnym wypadku produktów odnawianych (refurbished), pochodzących ze zwrotów, reklamacji, powystawowych itp.
8. Wykonawca zapewni dostawę do wskazanej lokalizacji w siedzibie Zamawiającego.
9. Wykonawca zobowiązany jest wykonać Przedmiot umowy z najwyższą starannością oraz zgodnie z obowiązującymi przepisami prawa w tym zakresie

## § 2

### Termin wykonania umowy

1. Strony ustalają termin realizacji Umowy, tj. wykonanie przedmiotu całości umowy wraz z wymaganą instalacją i konfiguracją w ciągu 30 dni od daty zawarcia Umowy.
2. Termin określony w ust. 1 może ulec zmianie w przypadkach wskazanych w § 11 Umowy. Zmiana terminu wymaga aneksu do Umowy w formie pisemnej pod rygorem nieważności
3. Potwierdzeniem realizacji zamówienia w terminie, o którym mowa w ust. 1 jest protokół odbioru podpisany przez obie Strony.

### § 3

#### Sposób realizacji przedmiotu umowy

1. Strony deklarują współpracę w celu realizacji Umowy. W szczególności Strony zobowiązane są do wzajemnego powiadamiania o ważnych okolicznościach mających lub mogących mieć wpływ na wykonanie Umowy, w tym na ewentualne opóźnienia.
2. Językiem Umowy i językiem stosowanym podczas jej realizacji jest język polski. Dotyczy to także całej komunikacji między Stronami.
3. Wykonawca jest uprawniony do powierzenia wykonania części przedmiotu Umowy podwykonawcom, przy czym Wykonawca ponosi odpowiedzialność za działanie podwykonawców jak za własne działania.
4. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
5. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
6. Przedmiot umowy zostanie dostarczony przez Wykonawcę do siedziby Zamawiającego oraz zainstalowany i uruchomiony z uwzględnieniem szczegółowych wymagań w tym zakresie zawartych w Załączniku nr 1 do SWZ (Szczegółowy opis przedmiotu zamówienia).
7. Wykonawca wyda Zamawiającemu instrukcje obsługi sprzętu i oprogramowania lub – jeśli są one udostępniane przez producenta w formie elektronicznej – przekaze adresy WWW, pod którymi można je pobrać.
8. Wykonawca jest zobowiązany do sporządzenia i przekazania najpóźniej w dniu odbioru dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i systemów (loginy, hasła, kody PIN itp.), jeśli takie zostały wprowadzone przez Wykonawcę.
9. Wykonawca zgłosi gotowość do odbioru z wyprzedzeniem co najmniej 3 dni roboczych.
10. Odbiór Przedmiotu Umowy odbędzie się w siedzibie Zamawiającego w obecności przedstawicieli obydwu Stron i polegać będzie na sprawdzeniu jego zgodności z wymaganiami SWZ, kompletności i stanu.
11. Odbiór Przedmiotu Umowy zostanie potwierdzony protokołem odbioru, podpisanym przez przedstawicieli Zamawiającego i Wykonawcy.
12. Protokół odbioru sporządzony zostanie w formie pisemnej, pod rygorem nieważności, w dwóch egzemplarzach, po jednym dla każdej ze Stron. O ile z Umowy lub przepisów prawa nie wynika inaczej, jedynie podpisany przez obie Strony Protokół odbioru jest podstawą do dokonania zapłaty wynagrodzenia. Zamawiający nie dopuszcza jednostronnych Protokołów odbioru wystawionych przez Wykonawcę.
13. Wykonawca oświadcza, że przedmiot umowy zostanie wykonany w zgodzie z prawem autorskim.
14. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.
15. Licencje na oprogramowanie zostaną udzielone bez ograniczeń czasowych, chyba, że w Załączniku nr 1 do SWZ (Szczegółowy Opis Przedmiotu Zamówienia) wskazano inaczej.
16. Oferowane oprogramowanie musi pochodzić z oficjalnego kanału dystrybucji producenta.
17. Zamawiający zastrzega sobie możliwość weryfikacji legalności oprogramowania bezpośrednio u producenta w przypadku, jeśli poweźmie wątpliwości co do legalności jego pochodzenia.



18. Korzyści i ciężary związane ze sprzętem oraz niebezpieczeństwo przypadkowej utraty lub uszkodzenia sprzętu przechodzą na Zamawiającego z chwilą wydania sprzętu Zamawiającemu i po podpisaniu protokołu, o którym mowa w ust. 11. Za dzień wydania sprzętu Zamawiającemu uważa się dzień, w którym sprzęt został odebrany przez Zamawiającego zgodnie z procedurą określoną w ust. 10 i dalszych.
19. Prace instalacyjne i konfiguracyjne towarzyszące dostawom muszą być przeprowadzone przez osoby posiadające kompetencje i doświadczenie w zakresie instalacji, konfiguracji i zarządzania danym urządzeniem lub oprogramowaniem (w zakresie odpowiadającym specyfice danego przedmiotu dostawy). Zamawiający wskazuje, że prawidłowa konfiguracja urządzeń i oprogramowania jest warunkiem odbioru przedmiotu umowy.
20. Przed rozpoczęciem prac związanych z realizacją zamówienia w zakresie instalowania i uruchomienia serwerów Wykonawca zobowiązany jest przedstawić Zamawiającemu stosowne dokumenty potwierdzające kwalifikację tych osób w zakresie posiadania certyfikatu wystawianego przez producenta oferowanych serwerów, na poziomie minimum specjalisty (ang. specialist/professional) lub wyższym dla osób przeprowadzających uruchomienie tych serwerów;
21. W celu uniknięcia wątpliwości przyjmuje się, że jeżeli Strony nie zdefiniowały danego działania niezbędnego do prawidłowej realizacji Umowy jako obowiązku Zamawiającego, Stroną zobowiązaną do wykonania takiego działania jest Wykonawca, jako podmiot profesjonalny. Powyższe ma zastosowanie w szczególności do elementów umożliwiających instalację i uruchomienie zakupionego sprzętu, np. kabli połączeniowych, zasilających, elementów montażowych, baterii itp.

#### § 4

#### Uwarunkowania wynagrodzenia

1. Wykonawca oświadcza, że:
  - 1) szczegółowo przeanalizował opis przedmiotu zamówienia opisany w SWZ oraz uzyskał przed złożeniem oferty przetargowej potrzebne informacje dotyczące zakresu zamówienia i warunków realizacji prac;
  - 2) przed złożeniem oferty przetargowej upewnił się co do jej prawidłowości i kompletności oraz stawek i cen podanych w ofercie.
2. Cena oferowana przez Wykonawcę obejmuje kompleksowe wykonanie przedmiotu zamówienia.
3. Strony zgodnie oświadczają, że wynagrodzenie obejmuje oraz pokrywa wszelkie koszty związane z realizacją przedmiotu zamówienia.
4. Zamawiający na podstawie art. 4 ustawy z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych zobowiązany jest do odbierania od Zleceniobiorcy ustrukturyzowanych faktur elektronicznych związanych z realizacją zamówień publicznych.
5. Zasady wystawiania faktur:
  - 1) Zamawiający upoważnia Wykonawcę do wystawiania faktury na:  
Nabywca Podmiot\_2 w strukturze logicznej FA(3): **Gmina Potok Górny, 23-423 Potok Górny 116, NIP 918-19-89-917**  
Odbiorca Podmiot\_3 w strukturze logicznej FA(3), Rola 8 – JST: **Urząd Gminy Potok Górny, 23-423 Potok Górny 116, NIP: 918-10-56-344, REGON: 000550864**
  - 2) Podstawą płatności wynagrodzenia z tytułu realizacji przedmiotu Umowy, będzie stanowiła ustrukturyzowana faktura elektroniczna wystawiona w Krajowym Systemie e-Faktur (KSeF).

- 3) Strony zgodnie postanawiają, iż faktura ustrukturyzowana, o której mowa powyżej jest uznana za doręczoną Zamawiającemu z chwilą nadania jej przez KSeF unikalnego numeru identyfikacyjnego, z wyłączeniem sytuacji awaryjnych, w których faktury zostały wystawione poza KSeF w przypadkach niedostępności KSeF tj. w trybie offline.
  - 4) W przypadku ogłoszonej przez właściwy organ niedostępności KSeF lub w innych przewidzianych prawem sytuacjach uniemożliwiających wystawienie faktury przy wykorzystaniu systemu, Wykonawca jest uprawniony do wystawienia faktury poza KSeF w przewidzianych trybach (tryb „offline”) zgodnie z obowiązującymi przepisami ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług.
  - 5) Wykonawca niezwłocznie po wystawieniu faktury w trybie, o którym mowa w pkt 4, udostępni ją Zamawiającemu poza KSeF w formie pliku PDF wraz z odpowiednimi kodami QR zgodnie z wymaganymi przepisami ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług.
  - 6) Wykonawca zobowiązuje się przekazać faktury wystawione w trybie offline do KSeF w terminach określonych przepisami.
  - 7) Po nadaniu numeru KSeF faktura jest traktowana jak doręczona zgodnie z obowiązującymi przepisami.
  - 8) Strony zgodnie potwierdzają, iż faktury wystawione zgodnie z powyższymi pkt 4-7 wywołują skutki prawne i rozliczeniowe jak faktury ustrukturyzowane wystawione w KSeF.
  - 9) Wykonawca zobowiązany jest do przekazywania informacji o wystawieniu faktury w Krajowym Systemie e-Faktur (KSeF) na adres e-mail: sekretariat@potokgorny.com.pl.
  - 10) Wykonawca jest uprawnione do przesyłania na ww. adres e-mail faktur wystawianych na skutek awarii Krajowego Systemu e-Faktur.
6. Zapłata faktury nastąpi z uwzględnieniem przepisów art. 108a ust. 1a ustawy o podatku od towarów i usług.
  7. Wykonawca jest zobowiązany podać na fakturze adnotację „mechanizm podzielonej płatności”.
  8. Strony zgodnie postanawiają, że warunkiem zapłaty w umówionym terminie za fakturę wystawioną przez czynnego podatnika VAT jest wskazanie przez Wykonawcę dla potrzeb dokonania zapłaty rachunku bankowego zawartego na dzień zlecenia przelewu w wykazie podmiotów, o którym mowa w art. 96b ust. 1 ustawy o VAT - Wykazie podmiotów zarejestrowanych jako podatnicy VAT, niezarejestrowanych oraz wykreślonych i przywróconych do rejestru VAT, najpóźniej na 5 dni roboczych przed wyznaczonym terminem płatności,
  9. W przypadku, w którym Wykonawca, dla potrzeb płatności, wskaże rachunek bankowy zawarty w powyższym Wykazie w terminie późniejszym, ustalony pierwotnie termin płatności ulega wydłużeniu i wynosi 5 dni roboczych od dnia wskazania rachunku ujawnionego ww. wykazie.

## § 5

### Wysokość wynagrodzenia

1. Wynagrodzenie za wykonanie przedmiotu Umowy strony ustaliły na podstawie ceny z oferty Wykonawcy. Jest to wynagrodzenie ryczałtowe za kompleksowe wykonanie przedmiotu zamówienia.
2. Ustalone w tej formie wynagrodzenie Zleceniobiorcy przedmiotu zamówienia wyraża się kwotą:  
Brutto: ..... zł;  
słownie zł.: ...../100  
w tym VAT: ..... zł;

słownie zł.: ..... /100

Netto: ..... zł

słownie zł.: ...../100

W tym:

- 1) Zakup serwera z oprogramowaniem typ I

Netto: ..... zł

słownie zł.:...../100

- 2) Zakup serwera z oprogramowaniem typ II

Netto: ..... zł

słownie zł.:...../100

- 3) Zakup i wdrożenie rozwiązania Network Access Control

Netto: ..... zł

słownie zł.:...../100

- 4) Zakup oprogramowania do archiwizacji i kategoryzacji logów

Netto: ..... zł

słownie zł.:...../100

- 5) Zakup oprogramowania do inwentaryzacji i ochrony przed wyciekami DLP

Netto: ..... zł

słownie zł.:...../100

3. Wykonawca zapoznał się szczegółowo z zakresem rzeczowym i zobowiązuje się wykonać przedmiot zamówienia w całości za umówioną cenę.
4. Wynagrodzenie będzie płatne powykonawczo przelewem w terminie do 30 dni od daty otrzymania prawidłowo wystawionej faktury VAT/rachunku. Wynagrodzenie będzie płatne na rachunek Wykonawcy wskazany na fakturze/ rachunku.
5. Za datę zapłaty Strony ustalają dzień obciążenia rachunku Zamawiającego.
6. Strony postanawiają, że rozliczenie za wykonanie umowy odbędzie się jedną fakturą po wykonaniu całości przedmiotu umowy.
7. Podpisany protokół odbioru stanowi potwierdzenie wykonania usługi i upoważnia Wykonawcę do wystawienia faktury.
8. Zamawiający zastrzega sobie prawo odmowy zapłaty faktury niezgodnej z zapisami niniejszej umowy lub przepisami powszechnie obowiązującymi
9. Termin płatności faktury, o której mowa w ust. 4 będzie liczony od prawidłowo wystawionej faktury.

## §6

### Gwarancja i rękojmia

1. Wykonawca udziela gwarancji na przedmiot umowy na zasadach opisanych w Szczegółowym Opisie Przedmiotu Zamówienia stanowiącym Załącznik nr 1 do niniejszej Umowy.
2. Okres gwarancji biegnie od dnia następnego po dniu podpisania protokołu odbioru końcowego przez Zamawiającego.
3. Gwarancja udzielona przez Wykonawcę nie wyłącza uprawnień Zamawiającego z tytułu



gwarancji udzielonych przez producentów sprzętu i oprogramowania, w szczególności jeżeli w SOPZ sformułowano warunki serwisu gwarancyjnego odnoszące się do gwarancji producenta. Warunki gwarancji Wykonawcy mają pierwszeństwo przed warunkami gwarancji udzielonymi przez producentów sprzętu i oprogramowania w zakresie, w jakim warunki gwarancji przyznają Zamawiającemu silniejszą ochronę.

4. Gwarancja udzielana jest w ramach wynagrodzenia.
5. W okresie gwarancji Wykonawca zapewnia serwis techniczny i nie może odmówić wymiany niesprawnej części na nową w przypadku, gdy jej naprawa nie gwarantuje prawidłowej pracy sprzętu, zgodnie z warunkami gwarancyjnymi.
6. Niezależnie od udzielonej gwarancji, wykonawca ponosi wobec Zamawiającego odpowiedzialność za wady fizyczne i prawne przedmiotu umowy z tytułu rękojmi w terminie i na zasadach określonych w ustawie Kodeks cywilny. Okres rękojmi równa się okresowi gwarancji.
7. Wykonawca ponosi wobec Zamawiającego odpowiedzialność za wady przedmiotu umowy z tytułu gwarancji jakości w terminie i na zasadach określonych w niniejszej Umowie, a w sprawach nieuregulowanych niniejszą umową przyjmuje się jako wiążące przepisy ustawy Kodeks cywilny.
8. Przez wadę należy rozumieć wadę fizyczną i prawną. Wada fizyczna rozumiana, jako jawne lub ukryte właściwości tkwiące w sprzęcie i oprogramowaniu stanowiących przedmiot umowy lub w jakimkolwiek ich elemencie, powodujące niemożność używania lub korzystania z przedmiotu umowy zgodnie z przeznaczeniem, a także obniżenie jakości, uszkodzenia lub usterki w przedmiocie umowy. Wada prawna rozumiana, jako sytuacja w której przedmiot umowy lub jakikolwiek element przedmiotu umowy nie stanowi własności Wykonawcy albo jeżeli jest obciążony prawem osoby trzeciej, a także inne wady prawne.
9. Zgłoszenie awarii lub wady następuje telefonicznie/faxem na numer telefonu/faxu..... lub na adres email: .....
10. W okresie objętym gwarancją/rękojmią Wykonawca zobowiązuje się do zapewnienia serwisu technicznego, nieodpłatnego usuwania usterek uszkodzonego sprzętu lub nieodpłatnej dostawy sprzętu wolnego od wad, na następujących warunkach:
  - 1) naprawy gwarancyjne urządzeń muszą być realizowane przez Producenta lub Autoryzowany Serwis Producenta.
  - 2) Gwarancja obejmuje bezpłatne naprawy, a w przypadku braku możliwości naprawy wymianę towaru lub jego podzespołu na nowy i ewentualnie poniesienie kosztów transportu;
  - 3) Wykonawca, w okresie gwarancyjnym, zapewni bezpłatny dojazd serwisanta do Zamawiającego, ewentualny bezpłatny transport sprzętu do i z serwisu.
  - 4) w okresie gwarancji serwis dostarczonego sprzętu będzie realizowany nieodpłatnie;
  - 5) W przypadku braku możliwości usunięcia zgłoszonej awarii w ciągu 7 dni roboczych Wykonawca zobowiązany jest do bezpłatnego dostarczenia i uruchomienia nowego sprzętu zastępczego o parametrach równoważnych, zgodnych z parametrami wynikającymi z opisu przedmiotu zamówienia (Załącznik nr 1 do SWZ), w przeciągu następnych 3 dni roboczych.
  - 6) Diagnostyka awarii zostanie przeprowadzona przez Wykonawcę.
  - 7) W przypadku wymiany sprzętu/towaru na nowy, okres jego gwarancji ulega odpowiednio wydłużeniu o czas wskazany w ust. 12.
  - 8) Jeżeli Wykonawca po wezwaniu do wymiany sprzętu/towaru lub usunięcia wad, nie dopełni obowiązku wymiany sprzętu/towaru na wolny od wad lub usunięcia wad w drodze

naprawy w wymaganym terminie Zamawiający jest uprawniony do usunięcia wad na ryzyko i koszt Wykonawcy bez konieczności uzyskania uprzedniej zgody sądu.

11. W przypadku wystąpienia konieczności naprawy sprzętu poza siedzibą Zamawiającego, wykonawca zapewni:
  - 1) odbiór na własny koszt wadliwego sprzętu,
  - 2) naprawę sprzętu w terminie do 7 dni roboczych od dnia zgłoszenia,
  - 3) dostawę naprawionego sprzętu na własny koszt.
12. Wykonawca na wniosek Zamawiającego dokona nieodpłatnej wymiany przedmiotu umowy na nowy o parametrach równoważnych, zgodnych z parametrami wynikającymi z opisu przedmiotu zamówienia (Załącznik nr 1 do SWZ) w terminie 7 dni roboczych od dnia zgłoszenia, gdy dany sprzęt po maksymalnie dwóch naprawach tego samego elementu wykaże dalsze wady w działaniu.

## § 9

### Kary umowne

1. W przypadku niewykonania lub nienależytego wykonania Umowy przez Wykonawcę
2. Zamawiający może naliczyć karę umowną w następujących przypadkach i wysokościach:
  - 1) za zwłokę w wykonaniu przedmiotu umowy w wysokości 0,2 % wynagrodzenia umownego brutto określonego w § 5 ust. 2, za każdy rozpoczęty dzień zwłoki;
  - 2) za zwłokę w usunięciu awarii lub wad przedmiotu umowy w okresie gwarancji lub rękojmi – w wysokości 0,2 % wynagrodzenia umownego brutto określonego w § 5 ust. 2, za każdy rozpoczęty dzień zwłoki liczonego od dnia wyznaczonego na usunięcie wad.
  - 3) za odstąpienie od Umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy w wysokości 20% całkowitego wynagrodzenia brutto, o którym mowa w § 5 ust. 2 Umowy.
3. Wykonawca może naliczyć karę umowną za odstąpienie od Umowy przez Wykonawcę z przyczyn leżących po stronie Zamawiającego w wysokości 20% całkowitego wynagrodzenia brutto, o którym mowa w §5 ust. 2 Umowy, z wyłączeniem przypadku, o jakim mowa w § 10 ust. 1 Umowy.
4. Kary umowne podlegają kumulacji z różnych tytułów, jednakże ich łączna wysokość, których mogą dochodzić Strony, nie może przekroczyć 30 % wartości Wynagrodzenia, o którym mowa w § 7 ust. 1 Umowy.
5. Zapłata kar umownych przez Wykonawcę nie zwalnia go z jakichkolwiek innych obowiązków i zobowiązań umownych.
6. Zamawiający może usunąć w zastępstwie Wykonawcy (bez konieczności uzyskania upoważnienia sądu), na jego koszt i ryzyko wady ujawnione w okresie gwarancji/rękojmi i nieusunięte w wyznaczonym terminie. Zamawiający ma obowiązek uprzedniego poinformowania Wykonawcy o zamiarze zastępczego usunięcia wad. Zastępcze usunięcie wady nie zwalnia z obowiązku zapłaty kar umownych, które naliczane są do momentu zastępczego usunięcia wady.
7. W przypadku wystąpienia szkody, której wysokość przekracza wysokość zastrzeżonych kar umownych Strony uprawnione są do dochodzenia odszkodowania przekraczającego wysokość kar umownych zasadach na ogólnych ustawy Kodeks cywilny.
8. Zamawiający ma prawo do potrącenia kar umownych z faktury przedłożonej do zapłaty przez Wykonawcę po uprzednim powiadomieniu Wykonawcy o podstawie i wysokości naliczonej kary umownej i wyznaczeniu mu 5 dniowego terminu zapłaty tej kary.

9. Powiadomienia o których mowa w ust. 8 Zamawiający może przekazać wedle własnego uznania:

- 1) w formie pisemnej listem poleconym za potwierdzeniem odbioru na adres .....,
- 2) w formie elektronicznej, o której mowa w art. 781 § 1 Kodeksu cywilnego na adres poczty elektronicznej: .....

10. Terminem otrzymania powiadomienia, o którym mowa w ust. 9 jest:

- 1) w przypadku powiadomienia złożonego w formie pisemnej – dzień jego odbioru wskazany na potwierdzeniu odbioru,
- 2) w przypadku powiadomienia złożonego w formie elektronicznej – dzień wysłania wiadomości zawierającej to powiadomienie na adres wskazany w ust. 9 pkt. 2).

## § 10

### Odstąpienie od Umowy

1. Zamawiającemu przysługuje prawo odstąpienia od Umowy 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 (zgodnie z art. 456 ust. 1 pkt 1 Ustawy Pzp).
2. Oprócz przypadków wymienionych w przepisach prawa, Zamawiającemu przysługiwać będzie prawo do odstąpienia od umowy z przyczyn leżących po stronie Wykonawcy, w terminie 7 dni od zaistnienia któregośkolwiek z poniższych zdarzeń:
  - a) Wykonawca mimo pisemnego wezwania przez Zamawiającego nie wykonuje zapisów Umowy zgodnie z jej postanowieniami lub w rażący sposób zaniedbuje bądź narusza zobowiązania umowne;
  - b) stwierdzenia w toku odbioru przedmiotu umowy, że przedmiot umowy zawiera wady i pomimo wyznaczenia terminu ich usunięcia Wykonawca ich nie poprawił lub nie przystąpił do ich usunięcia;
3. Wykonawcy przysługuje prawo do odstąpienia od Umowy w przypadku gdy Zamawiający nie wypełnia obowiązków wynikających z umowy pomimo pisemnego wezwania przez Wykonawcę w terminie 14 dni do wypełniania tych obowiązków Zamawiający nadal nie wypełnia, wówczas Wykonawca może odstąpić w terminie 30 dni od umowy.
4. Oświadczenie o odstąpieniu od umowy należy złożyć w formie pisemnej pod rygorem nieważności, w ciągu 14 dni od dnia powzięcia wiadomości o okolicznościach je uzasadniających i powinno zawierać uzasadnienie.
5. W przypadku odstąpienia od umowy, Wykonawca może żądać jedynie wynagrodzenia za wykonaną część umowy.
6. Strony zgodnie postanawiają, że odstąpienie od Umowy przez którąkolwiek ze Stron nie ma wpływu na obowiązek zapłaty zastrzeżonych kar umownych.

## § 11

### Zmiany Umowy

1. Oprócz przypadków, o których mowa w art. 454 i 455 ustawy – Prawo zamówień publicznych, strony dopuszczają możliwość wprowadzania zmiany umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy.



2. Zamawiający przewiduje możliwość wprowadzenia do Umowy zmian w przypadku zaistnienia okoliczności (technicznych, gospodarczych i tym podobnych), których nie można było przewidzieć w chwili zawarcia Umowy (z zastrzeżeniem, że zmiany te nie mogą powodować zmiany wysokości wynagrodzenia, ani obniżenia parametrów technicznych i jakościowych zaoferowanego przedmiotu zamówienia) na przykład:
  - 1) konieczność dostarczenia innego, niż określonego w Umowie urządzenia lub oprogramowania, niepowodująca zwiększenia ceny, spowodowana zakończeniem produkcji określonego w Umowie urządzenia/oprogramowania lub wycofania go z produkcji lub obrotu na terytorium Rzeczypospolitej Polskiej, posiadającego parametry nie gorsze od zaproponowanych przez Wykonawcę w ofercie;
  - 2) pojawienie się na rynku urządzenia producenta sprzętu nowszej generacji lub nowej wersji oprogramowania, o lepszych parametrach i/lub pozwalających na zaoszczędzenie kosztów eksploatacji pod warunkiem, że te zmiany nie spowodują zwiększenia ceny;
  - 3) w przypadku ujawnienia się powszechnie występujących wad oferowanego urządzenia Zamawiający dopuszcza zmianę w zakresie przedmiotu Umowy polegającą na zastąpieniu danego produktu produktem zastępczym, spełniającym wszelkie wymagania przewidziane w OPZ dla produktu zastępowanego, rekomendowanym przez producenta lub Wykonawcę w związku z ujawnieniem wad;
  - 4) zmiana oferowanych przez Wykonawcę urządzeń lub oprogramowania w sytuacji, gdy producent lub jego przedstawiciel na terytorium Rzeczypospolitej Polskiej (osoba trzecia) nie będzie mógł dostarczyć oferowanych przez Wykonawcę urządzeń lub oprogramowania w terminie wyznaczonym w Umowie.
  - 5) zmiany postanowień umowy w przypadku zmiany przepisów prawnych istotnych dla realizacji przedmiotu umowy, w tym m.in. w sytuacji określonej umową przewiduje się możliwość zmiany wysokości wynagrodzenia w przypadku zmiany stawki podatku od towarów i usług, – jeżeli zmiany te będą miały wpływ na koszty wykonania zamówienia przez Wykonawcę.
3. Zamawiający przewiduje możliwość dokonania zmiany terminu przewidzianego na zrealizowanie przedmiotu umowy w przypadku wydłużenia terminu realizacji grantów w projekcie „Cyberbezpieczny Samorząd”.
4. Zamawiający przewiduje możliwość dokonania zmiany terminu przewidzianego na zrealizowanie przedmiotu zamówienia w przypadku konieczności spowolnienia lub wstrzymania wykonywania niniejszej umowy, ze względu na:
  - 1) wstrzymanie realizacji przedmiotu umowy przez Zamawiającego ze względu na czynniki, których Zamawiający nie mógł przewidzieć;
  - 2) zmianę zakresu zamówienia;
  - 3) zmiany terminu realizacji Umowy ze względu na przyczyny będące konsekwencją zaistnienia zdarzeń spowodowanych przez „siłę wyższą” (tj. zdarzenia nagłe powstałe niezależnie od Stron Umowy, które są poza kontrolą Stron Umowy, na których czas trwania Strony nie mają jakiegokolwiek wpływu, a których zaistnienie uniemożliwia wypełnienie któregośkolwiek z zobowiązań wynikających z Umowy);
5. Warunkiem dokonania zmian, o których mowa powyżej jest:
  - 1) zainicjowanie zmian przez Wykonawcę lub Zamawiającego,
  - 2) uzasadnienie zmiany,
  - 3) forma pisemna pod rygorem nieważności.
6. Strony postanawiają, że w przypadku zmiany stawki podatku od towarów i usług – wynagrodzenie przewidziane niniejszą Umową ulegnie zmianie odpowiedniej do zmiany wysokości podatku od towarów i usług (ulegnie korekcie o wysokość zmiany podatku VAT),

przy czym powyższa zmiana będzie miała zastosowanie wyłącznie w odniesieniu do wynagrodzenia objętego fakturami wystawionymi po dacie wejścia w życie zmiany przepisów prawa wprowadzających nowe stawki podatku od towarów i usług.

7. Nie stanowi zmiany Umowy zmiana danych rejestrowych lub adresowych oraz ich danych kontaktowych.
8. Wszystkie powyższe zapisy stanowią katalog zmian, na które Zamawiający może wyrazić zgodę. Nie stanowią jednocześnie zobowiązania do wyrażenia takiej zgody.

## § 12

### Ochrona i przetwarzanie danych osobowych

1. W trakcie realizacji umowy Zamawiający oraz Wykonawca, będą przekazywać dane osobowe niezbędne do realizacji zamówienia. Na warunkach określonych niniejszą umową strony będą przetwarzać dane osobowe, poprzez wspólne ustalenie celów i sposobów przetwarzania tych danych.
2. Przetwarzanie danych osobowych będzie wykonywane przez okres trwania umowy. Dane osobowe będą przetwarzane przez Strony wyłącznie w celu wykonania przedmiotu niniejszej umowy.
3. Przetwarzanie danych osobowych będzie dotyczyć następujących kategorii danych osobowych:
  - a) Ze strony Zamawiającego: dane pracowników do kontaktu.
  - b) Ze strony Wykonawcy: dane pracowników wykonujących przedmiot niniejszej umowy.
4. Przetwarzanie będzie obejmować dane zwykłe takie jak: imię i nazwisko, nr telefonu, adres e-mail, stanowisko, tytuł zawodowy, firmę adres i NIP pracodawcy, firmę adres i NIP prowadzonej działalności.
5. Strony nie będą przetwarzać danych osobowych szczególnej kategorii o których mowa w art. 9 ust. 1 RODO.
6. Zamawiający oświadcza, że jest administratorem danych, o których mowa w ust. 3a.
7. Wykonawca oświadcza, że jest administratorem danych, o których mowa w ust. 3b.
8. Po wykonaniu przedmiotu zamówienia, Strony usuwają / zwracają udostępnione przez drugą stronę dane osobowe oraz usuwają wszelkie istniejące ich kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
9. Strony zobowiązują się:
  - a) przetwarzać powierzone im dane osobowe zgodnie z niniejszą umową, Rozporządzeniem, ustawą o ochronie danych osobowych oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą,
  - b) do zabezpieczenia przetwarzanych danych, poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia,
  - c) dołożyć należytej staranności przy przetwarzaniu udostępnianych danych osobowych,
  - d) do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy,
  - e) zapewnić zachowanie w tajemnicy (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.

10. Strony pomagają sobie w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia. Każda ze Stron niezwłocznie przekazuje żądanie osoby, której dane dotyczą, Administratorowi, który realizuje żądanie osoby.
11. Po stwierdzeniu naruszenia ochrony danych osobowych Strony bez zbędnej zwłoki zgłaszają je drugiemu administratorowi, nie później niż w ciągu 24 godzin od stwierdzenia naruszenia.
12. Strony, zgodnie z art. 28 ust. 3 pkt h Rozporządzenia mają prawo kontroli, czy środki zastosowane przy przetwarzaniu i zabezpieczeniu udostępnionych danych osobowych spełniają postanowienia umowy, w tym zlecenia jej wykonania audytorowi.
13. Strony będą realizować prawo kontroli w godzinach pracy Administratora informując o kontroli minimum 3 dni przed planowanym jej przeprowadzeniem.
14. Strony zobowiązują się do usunięcia uchybień stwierdzonych podczas kontroli w terminie nie dłuższym niż 7 dni.
15. Strony udostępnią na żądanie drugiego administratora wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.
16. Strony przyjmują, że Wykonawca może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Zamawiającego.
17. Podwykonawca, winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Wykonawcę.
18. Wykonawca ponosi pełną odpowiedzialność wobec Zamawiającego za działanie podwykonawcy w zakresie obowiązku ochrony danych.
19. Strony zobowiązują się do niezwłocznego poinformowania współadministratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania danych osobowych określonych w umowie, o jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych.
20. Strony zobowiązują się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od współadministratora oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
21. Strony oświadczają, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.
22. W sprawach nieuregulowanych niniejszym paragrafem, zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.

## **§ 10. Zachowanie poufności**

1. Strony umowy zobowiązują się do utrzymania w tajemnicy i nie przekazywania osobom trzecim, w tym także nieupoważnionym pracownikom, informacji i danych, które strony uzyskały w trakcie lub w związku z realizacją umowy, bez względu na sposób i formę ich utrwalenia lub przekazania, w szczególności w formie pisemnej, kserokopii, faksu i zapisu elektronicznego, o ile informacje takie nie są powszechnie znane, bądź obowiązek ich



ujawnienia nie wynika z obowiązujących przepisów, orzeczeń sądowych lub decyzji odpowiednich władz.

2. Zasadą poufności nie jest objęty fakt zawarcia oraz warunki umowy.
3. Ujawnienie przez którąkolwiek ze stron informacji poufnej, z zastrzeżeniem przepisu ust. 1, wymagać będzie każdorazowo pisemnej zgody drugiej strony, chyba, że są to informacje publicznie dostępne, a ich ujawnienie nie nastąpiło w wyniku naruszenia postanowień niniejszej umowy.
4. Obowiązek zachowania poufności nałożony jest na strony umowy bezterminowo.
5. Każda ze stron niezwłocznie poinformuje drugą stronę o ujawnieniu informacji, organie, któremu informacje zostały ujawnione oraz zakresie ujawnienia.

### § 13

#### Postanowienia końcowe

1. Wykonawca nie ma prawa dokonywać cesji, przeniesienia bądź obciążenia swoich praw lub obowiązków wynikających z Umowy bez uprzedniej pisemnej zgody Zamawiającego, udzielonej na piśmie pod rygorem nieważności.
2. Wszelkie spory będą poddane pod rozstrzygnięcie sądu powszechnego właściwego dla siedziby Zamawiającego.
3. W sprawach nie uregulowanych zastosowanie mają przepisy Ustawy, ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny oraz inne mające związek z przedmiotową Umową.
4. Wszelkie zmiany Umowy, jej uzupełnienie lub oświadczenia z nią związane wymagają formy pisemnej pod rygorem nieważności.
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, jeden dla Wykonawcy, jeden dla Zamawiającego.
6. Integralną część Umowy stanowią następujące Załączniki:
  - 1) Specyfikacja Warunków Zamówienia.
  - 2) Oferta Wykonawcy.



**UMOWA NR .../2026**

zawarta w dniu .....**2026 r.** w Potoku Górnym pomiędzy:  
**Gminą Potok Górny** z siedzibą w **Potok Górny 116, 23-423 Potok Górny**  
zwaną dalej „**Zamawiającym**”,

reprezentowaną w niniejszej Umowie przez:

**Pan Stanisław Dyjak** – Wójt Gminy Potok Górny  
przy kontrasygnacie Skarbnika Gminy Potok Górny – **Pani Aurelii Ćwikła**  
a

\*gdy kontrahentem jest spółka prawa handlowego:

spółką pod firmą „...” z siedzibą w ... (wpisać tylko nazwę miasta/miejscowości),  
ul. ...., ..... (wpisać adres), wpisaną do Rejestru Przedsiębiorców Krajowego  
Rejestru Sądowego pod numerem KRS ....., NIP ....., REGON  
....., zwaną dalej „Wykonawcą”, reprezentowaną przez .....<sup>1</sup>/reprezentowaną  
przez ... działającą/-ego na podstawie pełnomocnictwa, stanowiącego załącznik do umowy<sup>2</sup>,

\*gdy kontrahentem jest osoba fizyczna prowadząca działalność gospodarczą:

Panią/Panem ....., prowadzącą/-ym działalność gospodarczą pod firmą „...” zamieszkałym w  
... (wpisać tylko nazwę miasta/miejscowości), ul. ...., ..... (wpisać adres), NIP  
....., REGON ....., , zwaną/-ym dalej „Wykonawcą”, reprezentowaną/-ym przez ...  
działającą/-ego na podstawie pełnomocnictwa, stanowiącego załącznik do umowy<sup>3</sup>,  
wspólnie zwanymi dalej „Stronami”.

Strony oświadczają, że niniejsza umowa, zwana dalej „umową”, została zawarta  
w wyniku udzielenia zamówienia publicznego w trybie podstawowym, zgodnie  
z przepisami ustawy z dnia 11 września 2019 r. (Dz. U. z 2024 r. poz. 1320 z późn. zm.) – Prawo  
zamówień publicznych.

**Oświadczenia Stron**

1. Strony oświadczają, że niniejsza umowa, zwana dalej „umową”, została zawarta w wyniku przeprowadzonego postępowania o udzielenie zamówienia publicznego w trybie podstawowym zgodnie z art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320 t. j. z późn. zm.),
2. Zamawiający i Wykonawca zobowiązują się współdziałać przy wykonaniu umowy w sprawie zamówienia publicznego w celu należytej realizacji zamówienia.

**§ 1****Przedmiot umowy**

1. Przedmiotem zamówienia jest realizacja zadania pn. „**Zakup sprzętu IT wraz z oprogramowaniem w ramach projektu Zwiększenie cyberbezpieczeństwa Gminy Potok Górny**” w zakresie **Część 2 Dostawa przełączników sieciowych, serwera NAS oraz UPS - a.**
2. Zadanie realizowane jest w związku z realizacją projektu pn. „**Zwiększenie cyberbezpieczeństwa Gminy Potok Górny**”, współfinansowanego ze środków Unii

<sup>1</sup> Jeżeli przy zawarciu umowy działa osoba/-y pełniący/-e funkcję organu (członka organu) lub prokurent spółki.  
<sup>2</sup> Jeżeli przy zawarciu umowy działa pełnomocnik spółki.  
<sup>3</sup> Jeżeli przy zawarciu umowy działa pełnomocnik tej osoby.



Europejskiej i budżetu państwa w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Priorytetu II Zaawansowane usługi cyfrowe, Działania 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.01-001/23/2520/ FERC.02.02-CS.01-001/23/2024.

3. Przedmiotem Umowy jest:

- 1) Zakup serwer NAS - 2 kpl.
- 2) Zakup przełącznika sieciowego zarządzalnego - 3 szt
- 3) Zakup UPS - 1 szt.

4. W ramach realizacji zamówienia Wykonawca zobowiązuje się w szczególności do:

- 1) dostawy sprzętu informatycznego określonego w SOPZ,
  - 2) instalacji, konfiguracji oraz uruchomienia dostarczonych urządzeń i systemów,
  - 3) wdrożenia sprzętu informatycznego zgodnie z wymaganiami określonymi w SOPZ,
  - 4) integracji dostarczonych rozwiązań z istniejącą infrastrukturą informatyczną Zamawiającego, jeżeli jest to wymagane,
  - 5) przeprowadzenia szkolenia administratorów Zamawiającego w zakresie obsługi dostarczonych systemów, jeżeli wymaganie takie wynika z SOPZ,
  - 6) przekazania dokumentacji technicznej oraz powdrożeniowej dotyczącej dostarczonych urządzeń i systemów.
5. Szczegółowy zakres zamówienia określony jest w Specyfikacji Warunków Zamówienia oraz w załączonym do SWZ Szczegółowym Opisie Przedmiotu Zamówienia Załącznik nr 1 do SWZ.
6. Dostarczany przedmiot umowy musi być fabrycznie nowy, nieużywany, nieuszkodzony i nieobciążony prawami osób trzecich oraz muszą pochodzić z oficjalnego kanału dystrybucyjnego w UE.
7. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą się znajdować się na liście „end-of-sale” oraz „end-of-support” producenta, nie dopuszcza w żadnym wypadku produktów odnawianych (refurbished), pochodzących ze zwrotów, reklamacji, powystawowych itp.
8. Wykonawca zapewni dostawę do wskazanej lokalizacji w siedzibie Zamawiającego.
9. Wykonawca zobowiązany jest wykonać Przedmiot umowy z najwyższą starannością oraz zgodnie z obowiązującymi przepisami prawa w tym zakresie

## § 2

### Termin wykonania umowy

1. Strony ustalają termin realizacji Umowy, tj. wykonanie całości przedmiotu umowy wraz z wymaganą instalacją i konfiguracją w ciągu 30 dni od daty zawarcia Umowy.
2. Termin określony w ust. 1 może ulec zmianie w przypadkach wskazanych w § 11 Umowy. Zmiana terminu wymaga aneksu do Umowy w formie pisemnej pod rygorem nieważności
3. Potwierdzeniem realizacji zamówienia w terminie, o którym mowa w ust. 1 jest protokół odbioru podpisany przez obie Strony.

### § 3

#### Sposób realizacji przedmiotu umowy

1. Strony deklarują współpracę w celu realizacji Umowy. W szczególności Strony zobowiązane są do wzajemnego powiadamiania o ważnych okolicznościach mających lub mogących mieć wpływ na wykonanie Umowy, w tym na ewentualne opóźnienia.
2. Językiem Umowy i językiem stosowanym podczas jej realizacji jest język polski. Dotyczy to także całej komunikacji między Stronami.
3. Wykonawca jest uprawniony do powierzenia wykonania części przedmiotu Umowy podwykonawcom, przy czym Wykonawca ponosi odpowiedzialność za działanie podwykonawców jak za własne działania.
4. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
5. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
6. Przedmiot umowy zostanie dostarczony przez Wykonawcę do siedziby Zamawiającego oraz zainstalowany i uruchomiony z uwzględnieniem szczegółowych wymagań w tym zakresie zawartych w Załączniku nr 1 do SWZ (Szczegółowy opis przedmiotu zamówienia).
7. Wykonawca wyda Zamawiającemu instrukcje obsługi sprzętu i oprogramowania lub – jeśli są one udostępniane przez producenta w formie elektronicznej – prześle adresy WWW, pod którymi można je pobrać.
8. Wykonawca jest zobowiązany do sporządzenia i przekazania najpóźniej w dniu odbioru dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i systemów (loginy, hasła, kody PIN itp.), jeśli takie zostały wprowadzone przez Wykonawcę.
9. Wykonawca zgłosi gotowość do odbioru z wyprzedzeniem co najmniej 3 dni roboczych.
10. Odbiór Przedmiotu Umowy odbędzie się w siedzibie Zamawiającego w obecności przedstawicieli obydwu Stron i polegać będzie na sprawdzeniu jego zgodności z wymaganiami SWZ, kompletności i stanu.
11. Odbiór Przedmiotu Umowy zostanie potwierdzony protokołem odbioru, podpisanym przez przedstawicieli Zamawiającego i Wykonawcy.
12. Protokół odbioru sporządzony zostanie w formie pisemnej, pod rygorem nieważności, w dwóch egzemplarzach, po jednym dla każdej ze Stron. O ile z Umowy lub przepisów prawa nie wynika inaczej, jedynie podpisany przez obie Strony Protokół odbioru jest podstawą do dokonania zapłaty wynagrodzenia. Zamawiający nie dopuszcza jednostronnych Protokołów odbioru wystawionych przez Wykonawcę.
13. Wykonawca oświadcza, że przedmiot umowy zostanie wykonany w zgodzie z prawem autorskim.
14. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.
15. Licencje na oprogramowanie zostaną udzielone bez ograniczeń czasowych, chyba, że w Załączniku nr 1 do SWZ (Szczegółowy Opis Przedmiotu Zamówienia) wskazano inaczej.
16. Zamawiający zastrzega sobie możliwość weryfikacji legalności oprogramowania bezpośrednio u producenta w przypadku, jeśli poweźmie wątpliwości co do legalności jego pochodzenia.

17. Korzyści i ciężary związane ze sprzętem oraz niebezpieczeństwo przypadkowej utraty lub uszkodzenia sprzętu przechodzą na Zamawiającego z chwilą wydania sprzętu Zamawiającemu i po podpisaniu protokołu, o którym mowa w ust. 11. Za dzień wydania sprzętu Zamawiającemu uważa się dzień, w którym sprzęt został odebrany przez Zamawiającego zgodnie z procedurą określoną w ust. 10 i dalszych.
18. Prace instalacyjne i konfiguracyjne towarzyszące dostawom muszą być przeprowadzone przez osoby posiadające kompetencje i doświadczenie w zakresie instalacji, konfiguracji i zarządzania danym urządzeniem lub oprogramowaniem (w zakresie odpowiadającym specyfice danego przedmiotu dostawy). Zamawiający wskazuje, że prawidłowa konfiguracja urządzeń i oprogramowania jest warunkiem odbioru przedmiotu umowy.
19. W celu uniknięcia wątpliwości przyjmuje się, że jeżeli Strony nie zdefiniowały danego działania niezbędnego do prawidłowej realizacji Umowy jako obowiązku Zamawiającego, Stroną zobowiązaną do wykonania takiego działania jest Wykonawca, jako podmiot profesjonalny. Powyższe ma zastosowanie w szczególności do elementów umożliwiających instalację i uruchomienie zakupionego sprzętu, np. kabli połączeniowych, zasilających, elementów montażowych, baterii itp.

#### § 4

#### Uwarunkowania wynagrodzenia

1. Wykonawca oświadcza, że:
  - 1) szczegółowo przeanalizował opis przedmiotu zamówienia opisany w SWZ oraz uzyskał przed złożeniem oferty przetargowej potrzebne informacje dotyczące zakresu zamówienia i warunków realizacji prac;
  - 2) przed złożeniem oferty przetargowej upewnił się co do jej prawidłowości i kompletności oraz stawek i cen podanych w ofercie.
2. Cena oferowana przez Wykonawcę obejmuje kompleksowe wykonanie przedmiotu zamówienia.
3. Strony zgodnie oświadczają, że wynagrodzenie obejmuje oraz pokrywa wszelkie koszty związane z realizacją przedmiotu zamówienia.
4. Zamawiający na podstawie art. 4 ustawy z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych zobowiązany jest do odbierania od Zleceniobiorcy ustrukturyzowanych faktur elektronicznych związanych z realizacją zamówień publicznych.
5. Zasady wystawiania faktur:
  - 1) Zamawiający upoważnia Wykonawcę do wystawiania faktury na:  
Nabywca Podmiot\_2 w strukturze logicznej FA(3): **Gmina Potok Górny, 23-423 Potok Górny 116, NIP 918-19-89-917**  
Odbiorca Podmiot\_3 w strukturze logicznej FA(3), Rola 8 – JST: **Urząd Gminy Potok Górny, 23-423 Potok Górny 116, NIP: 918-10-56-344, REGON: 000550864**
  - 2) Podstawą płatności wynagrodzenia z tytułu realizacji przedmiotu Umowy, będzie stanowiła ustrukturyzowana faktura elektroniczna wystawiona w Krajowym Systemie e-Faktur (KSeF).
  - 3) Strony zgodnie postanawiają, iż faktura ustrukturyzowana, o której mowa powyżej jest uznana za doręczoną Zamawiającemu z chwilą nadania jej przez KSeF unikalnego numeru identyfikacyjnego, z wyłączeniem sytuacji awaryjnych, w których faktury zostały wystawione poza KSeF w przypadkach niedostępności KSeF tj. w trybie offline.
  - 4) W przypadku ogłoszonej przez właściwy organ niedostępności KSeF lub w innych przewidzianych prawem sytuacjach uniemożliwiających wystawienie faktury przy



wykorzystaniu systemu, Wykonawca jest uprawniony do wystawienia faktury poza KSeF w przewidzianych trybach (tryb „offline”) zgodnie z obowiązującymi przepisami ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług.

- 5) Wykonawca niezwłocznie po wystawieniu faktury w trybie, o którym mowa w pkt 4, udostępni ją Zamawiającemu poza KSeF w formie pliku PDF wraz z odpowiednimi kodami QR zgodnie z wymaganymi przepisami ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług.
  - 6) Wykonawca zobowiązuje się przekazać faktury wystawione w trybie offline do KSeF w terminach określonych przepisami.
  - 7) Po nadaniu numeru KSeF faktura jest traktowana jak doręczona zgodnie z obowiązującymi przepisami.
  - 8) Strony zgodnie potwierdzają, iż faktury wystawione zgodnie z powyższymi pkt 4-7 wywołują skutki prawne i rozliczeniowe jak faktury ustrukturyzowane wystawione w KSeF.
  - 9) Wykonawca zobowiązany jest do przekazywania informacji o wystawieniu faktury w Krajowym Systemie e-Faktur (KSeF) na adres e-mail: sekretariat@potokgorny.com.pl.
  - 10) Wykonawca jest uprawnione do przysyłania na ww. adres e-mail faktur wystawianych na skutek awarii Krajowego Systemu e-Faktur.
6. Zapłata faktury nastąpi z uwzględnieniem przepisów art. 108a ust. 1a ustawy o podatku od towarów i usług.
  7. Wykonawca jest zobowiązany podać na fakturze adnotację „mechanizm podzielonej płatności”.
  8. Strony zgodnie postanawiają, że warunkiem zapłaty w umówionym terminie za fakturę wystawioną przez czynnego podatnika VAT jest wskazanie przez Wykonawcę dla potrzeb dokonania zapłaty rachunku bankowego zawartego na dzień zlecenia przelewu w wykazie podmiotów, o którym mowa w art. 96b ust. 1 ustawy o VAT - Wykazie podmiotów zarejestrowanych jako podatnicy VAT, niezarejestrowanych oraz wykreślonych i przywróconych do rejestru VAT, najpóźniej na 5 dni roboczych przed wyznaczonym terminem płatności,
  9. W przypadku, w którym Wykonawca, dla potrzeb płatności, wskaże rachunek bankowy zawarty w powyższym Wykazie w terminie późniejszym, ustalony pierwotnie termin płatności ulega wydłużeniu i wynosi 5 dni roboczych od dnia wskazania rachunku ujawnionego ww. wykazie.

## § 5

### Wysokość wynagrodzenia

1. Wynagrodzenie za wykonanie przedmiotu Umowy strony ustaliły na podstawie ceny z oferty Wykonawcy. Jest to wynagrodzenie ryczałtowe za kompleksowe wykonanie przedmiotu zamówienia.
2. Ustalone w tej formie wynagrodzenie Zleceniobiorcy przedmiotu zamówienia wyraża się kwotą:  
Brutto: ..... zł;  
słownie zł.: ...../100  
w tym VAT: ..... zł;  
słownie zł.: ..... /100  
Netto: ..... zł  
słownie zł.: ...../100

W tym:

## 1) Zakup serwer NAS - 2 kpl.

Netto: ..... zł

słownie zł.:...../100

## 2) Zakup przełącznika sieciowego zarządzalnego - 3 szt.

Netto: ..... zł

słownie zł.:...../100

## 3) Zakup UPS

Netto: ..... zł

słownie zł.:...../100

3. Wykonawca zapoznał się szczegółowo z zakresem rzeczowym i zobowiązuje się wykonać przedmiot zamówienia w całości za umówioną cenę.
4. Wynagrodzenie będzie płatne powykonawczo przelewem w terminie do 30 dni od daty otrzymania prawidłowo wystawionej faktury VAT/rachunku. Wynagrodzenie będzie płatne na rachunek Wykonawcy wskazany na fakturze/ rachunku.
5. Za datę zapłaty Strony ustalają dzień obciążenia rachunku Zamawiającego.
6. Strony postanawiają, że rozliczenie za wykonanie umowy odbędzie się jedną fakturą po wykonaniu całości przedmiotu umowy.
7. Podpisany protokół odbioru stanowi potwierdzenie wykonania usługi i upoważnia Wykonawcę do wystawienia faktury.
8. Zamawiający zastrzega sobie prawo odmowy zapłaty faktury niezgodnej z zapisami niniejszej umowy lub przepisami powszechnie obowiązującymi
9. Termin płatności faktury, o której mowa w ust. 4 będzie liczony od prawidłowo wystawionej faktury.

**§6****Gwarancja i rękojmia**

1. Wykonawca udziela gwarancji na przedmiot umowy na zasadach opisanych w Szczegółowym Opisie Przedmiotu Zamówienia stanowiącym Załącznik nr 1 do niniejszej Umowy.
2. Okres gwarancji biegnie od dnia następnego po dniu podpisania protokołu odbioru końcowego przez Zamawiającego.
3. Gwarancja udzielona przez Wykonawcę nie wyłącza uprawnień Zamawiającego z tytułu gwarancji udzielonych przez producentów sprzętu i oprogramowania, w szczególności jeżeli w SOPZ sformułowano warunki serwisu gwarancyjnego odnoszące się do gwarancji producenta. Warunki gwarancji Wykonawcy mają pierwszeństwo przed warunkami gwarancji udzielonymi przez producentów sprzętu i oprogramowania w zakresie, w jakim warunki gwarancji przyznają Zamawiającemu silniejszą ochronę.
4. Gwarancja udzielana jest w ramach wynagrodzenia.
5. W okresie gwarancji Wykonawca zapewnia serwis techniczny i nie może odmówić wymiany niesprawnej części na nową w przypadku, gdy jej naprawa nie gwarantuje prawidłowej pracy sprzętu, zgodnie z warunkami gwarancyjnymi.
6. Niezależnie od udzielonej gwarancji, wykonawca ponosi wobec Zamawiającego odpowiedzialność za wady fizyczne i prawne przedmiotu umowy z tytułu rękojmi w terminie i na zasadach określonych w ustawie Kodeks cywilny. Okres rękojmi równa się okresowi gwarancji.

7. Wykonawca ponosi wobec Zamawiającego odpowiedzialność za wady przedmiotu umowy z tytułu gwarancji jakości w terminie i na zasadach określonych w niniejszej Umowie, a w sprawach nieuregulowanych niniejszą umową przyjmuje się jako wiążące przepisy ustawy Kodeks cywilny.
8. Przez wadę należy rozumieć wadę fizyczną i prawną. Wada fizyczna rozumiana, jako jawne lub ukryte właściwości tkwiące w sprzęcie i oprogramowaniu stanowiących przedmiot umowy lub w jakimkolwiek ich elemencie, powodujące niemożność używania lub korzystania z przedmiotu umowy zgodnie z przeznaczeniem, a także obniżenie jakości, uszkodzenia lub usterki w przedmiocie umowy. Wada prawna rozumiana, jako sytuacja w której przedmiot umowy lub jakiegokolwiek element przedmiotu umowy nie stanowi własności Wykonawcy albo jeżeli jest obciążony prawem osoby trzeciej, a także inne wady prawne.
9. Zgłoszenie awarii lub wady następuje telefonicznie/faxem na numer telefonu/faxu..... lub na adres email: .....
10. W okresie objętym gwarancją/rękojmią Wykonawca zobowiązuje się do zapewnienia serwisu technicznego, nieodpłatnego usuwania usterek uszkodzonego sprzętu lub nieodpłatnej dostawy sprzętu wolnego od wad, na następujących warunkach:
  - 1) naprawy gwarancyjne urządzeń muszą być realizowane przez Producenta lub Autoryzowany Serwis Producenta.
  - 2) Gwarancja obejmuje bezpłatne naprawy, a w przypadku braku możliwości naprawy wymianę towaru lub jego podzespołu na nowy i ewentualnie poniesienie kosztów transportu;
  - 3) Wykonawca, w okresie gwarancyjnym, zapewni bezpłatny dojazd serwisanta do Zamawiającego, ewentualny bezpłatny transport sprzętu do i z serwisu.
  - 4) w okresie gwarancji serwis dostarczonego sprzętu będzie realizowany nieodpłatnie;
  - 5) W przypadku braku możliwości usunięcia zgłoszonej awarii w ciągu 7 dni roboczych Wykonawca zobowiązany jest do bezpłatnego dostarczenia i uruchomienia nowego sprzętu zastępczego o parametrach równoważnych, zgodnych z parametrami wynikającymi z opisu przedmiotu zamówienia (Załącznik nr 1 do SWZ), w przeciągu następnych 3 dni roboczych.
  - 6) Diagnostyka awarii zostanie przeprowadzona przez Wykonawcę.
  - 7) W przypadku wymiany sprzętu/towaru na nowy, okres jego gwarancji ulega odpowiednio wydłużeniu o czas wskazany w ust. 12.
  - 8) Jeżeli Wykonawca po wezwaniu do wymiany sprzętu/towaru lub usunięcia wad, nie dopełnił obowiązku wymiany sprzętu/towaru na wolny od wad lub usunięcia wad w drodze naprawy w wymaganym terminie Zamawiający jest uprawniony do usunięcia wad na ryzyko i koszt Wykonawcy bez konieczności uzyskania uprzedniej zgody sądu.
11. W przypadku wystąpienia konieczności naprawy sprzętu poza siedzibą Zamawiającego, wykonawca zapewni:
  - 1) odbiór na własny koszt wadliwego sprzętu,
  - 2) naprawę sprzętu w terminie do 7 dni roboczych od dnia zgłoszenia,
  - 3) dostawę naprawionego sprzętu na własny koszt.
12. Wykonawca na wniosek Zamawiającego dokona nieodpłatnej wymiany przedmiotu umowy na nowy o parametrach równoważnych, zgodnych z parametrami wynikającymi z opisu przedmiotu zamówienia (Załącznik nr 1 do SWZ) w terminie 7 dni roboczych od dnia zgłoszenia, gdy dany sprzęt po maksymalnie dwóch naprawach tego samego elementu wykaże dalsze wady w działaniu.



## § 9

### Kary umowne

1. W przypadku niewykonania lub nienależytego wykonania Umowy przez Wykonawcę
2. Zamawiający może naliczyć karę umowną w następujących przypadkach i wysokościach:
  - 1) za zwłokę w wykonaniu przedmiotu umowy w wysokości 0,2 % wynagrodzenia umownego brutto określonego w § 5 ust. 2, za każdy rozpoczęty dzień zwłoki;
  - 2) za zwłokę w usunięciu awarii lub wad przedmiotu umowy w okresie gwarancji lub rękojmi – w wysokości 0,2 % wynagrodzenia umownego brutto określonego w § 5 ust. 2, za każdy rozpoczęty dzień zwłoki liczonego od dnia wyznaczonego na usunięcie wad.
  - 3) za odstąpienie od Umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy w wysokości 20% całkowitego wynagrodzenia brutto, o którym mowa w § 5 ust. 2 Umowy.
3. Wykonawca może naliczyć karę umowną za odstąpienie od Umowy przez Wykonawcę z przyczyn leżących po stronie Zamawiającego w wysokości 20% całkowitego wynagrodzenia brutto, o którym mowa w § 5 ust. 2 Umowy, z wyłączeniem przypadku, o jakim mowa w § 10 ust. 1 Umowy.
4. Kary umowne podlegają kumulacji z różnych tytułów, jednakże ich łączna wysokość, których mogą dochodzić Strony, nie może przekroczyć 30 % wartości Wynagrodzenia, o którym mowa w § 7 ust. 1 Umowy.
5. Zapłata kar umownych przez Wykonawcę nie zwalnia go z jakichkolwiek innych obowiązków i zobowiązań umownych.
6. Zamawiający może usunąć w zastępstwie Wykonawcy (bez konieczności uzyskania upoważnienia sądu), na jego koszt i ryzyko wady ujawnione w okresie gwarancji/rękojmi i nieusunięte w wyznaczonym terminie. Zamawiający ma obowiązek uprzedniego poinformowania Wykonawcy o zamiarze zastępczego usunięcia wad. Zastępcze usunięcie wady nie zwalnia z obowiązku zapłaty kar umownych, które naliczane są do momentu zastępczego usunięcia wady.
7. W przypadku wystąpienia szkody, której wysokość przekracza wysokość zastrzeżonych kar umownych Strony uprawnione są do dochodzenia odszkodowania przekraczającego wysokość kar umownych zasadach na ogólnych ustawy Kodeks cywilny.
8. Zamawiający ma prawo do potrącenia kar umownych z faktury przedłożonej do zapłaty przez Wykonawcę po uprzednim powiadomieniu Wykonawcy o podstawie i wysokości naliczonej kary umownej i wyznaczeniu mu 5 dniowego terminu zapłaty tej kary.
9. Powiadomienia o których mowa w ust. 8 Zamawiający może przekazać wedle własnego uznania:
  - 1) w formie pisemnej listem poleconym za potwierdzeniem odbioru na adres .....,
  - 2) w formie elektronicznej, o której mowa w art. 781 § 1 Kodeksu cywilnego na adres poczty elektronicznej: .....
10. Terminem otrzymania powiadomienia, o którym mowa w ust. 9 jest:
  - 1) w przypadku powiadomienia złożonego w formie pisemnej – dzień jego odbioru wskazany na potwierdzeniu odbioru,
  - 2) w przypadku powiadomienia złożonego w formie elektronicznej – dzień wysłania wiadomości zawierającej to powiadomienie na adres wskazany w ust. 9 pkt. 2).

## Odstąpienie od Umowy

1. Zamawiającemu przysługuje prawo odstąpienia od Umowy 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 (zgodnie z art. 456 ust. 1 pkt 1 Ustawy Pzp).
2. Oprócz przypadków wymienionych w przepisach prawa, Zamawiającemu przysługiwać będzie prawo do odstąpienia od umowy z przyczyn leżących po stronie Wykonawcy, w terminie 7 dni od zaistnienia któregośkolwiek z poniższych zdarzeń:
  - a) Wykonawca mimo pisemnego wezwania przez Zamawiającego nie wykonuje zapisów Umowy zgodnie z jej postanowieniami lub w rażący sposób zaniedbuje bądź narusza zobowiązania umowne;
  - b) stwierdzenia w toku odbioru przedmiotu umowy, że przedmiot umowy zawiera wady i pomimo wyznaczenia terminu ich usunięcia Wykonawca ich nie poprawił lub nie przystąpił do ich usunięcia;
3. Wykonawcy przysługuje prawo do odstąpienia od Umowy w przypadku gdy Zamawiający nie wypełnia obowiązków wynikających z umowy pomimo pisemnego wezwania przez Wykonawcę w terminie 14 dni do wypełniania tych obowiązków Zamawiający nadal nie wypełnia, wówczas Wykonawca może odstąpić w terminie 30 dni od umowy.
4. Oświadczenie o odstąpieniu od umowy należy złożyć w formie pisemnej pod rygorem nieważności, w ciągu 14 dni od dnia powzięcia wiadomości o okolicznościach je uzasadniających i powinno zawierać uzasadnienie.
5. W przypadku odstąpienia od umowy, Wykonawca może żądać jedynie wynagrodzenia za wykonaną część umowy.
6. Strony zgodnie postanawiają, że odstąpienie od Umowy przez którąkolwiek ze Stron nie ma wpływu na obowiązek zapłaty zastrzeżonych kar umownych.

## § 11

### Zmiany Umowy

1. Oprócz przypadków, o których mowa w art. 454 i 455 ustawy – Prawo zamówień publicznych, strony dopuszczają możliwość wprowadzania zmiany umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy.
2. Zamawiający przewiduje możliwość wprowadzenia do Umowy zmian w przypadku zaistnienia okoliczności (technicznych, gospodarczych i tym podobnych), których nie można było przewidzieć w chwili zawarcia Umowy (z zastrzeżeniem, że zmiany te nie mogą powodować zmiany wysokości wynagrodzenia, ani obniżenia parametrów technicznych i jakościowych zaoferowanego przedmiotu zamówienia) na przykład:
  - 1) konieczność dostarczenia innego, niż określonego w Umowie urządzenia lub oprogramowania, niepowodująca zwiększenia ceny, spowodowana zakończeniem produkcji określonego w Umowie urządzenia/oprogramowania lub wycofania go z produkcji lub obrotu na terytorium Rzeczypospolitej Polskiej, posiadającego parametry nie gorsze od zaproponowanych przez Wykonawcę w ofercie;
  - 2) pojawienie się na rynku urządzenia producenta sprzętu nowszej generacji lub nowej wersji oprogramowania, o lepszych parametrach i/lub pozwalających na zaoszczędzenie kosztów eksploatacji pod warunkiem, że te zmiany nie spowodują zwiększenia ceny;
  - 3) w przypadku ujawnienia się powszechnie występujących wad oferowanego urządzenia Zamawiający dopuszcza zmianę w zakresie przedmiotu Umowy polegającą na zastąpieniu

danego produktu produktem zastępczym, spełniającym wszelkie wymagania przewidziane w SOPZ dla produktu zastępowanego, rekomendowanym przez producenta lub Wykonawcę w związku z ujawnieniem wad;

- 4) zmiana oferowanych przez Wykonawcę urządzeń lub oprogramowania w sytuacji, gdy producent lub jego przedstawiciel na terytorium Rzeczypospolitej Polskiej (osoba trzecia) nie będzie mógł dostarczyć oferowanych przez Wykonawcę urządzeń lub oprogramowania w terminie wyznaczonym w Umowie.
  - 5) zmiany postanowień umowy w przypadku zmiany przepisów prawnych istotnych dla realizacji przedmiotu umowy, w tym m.in. w sytuacji określonej umową przewiduje się możliwość zmiany wysokości wynagrodzenia w przypadku zmiany stawki podatku od towarów i usług, – jeżeli zmiany te będą miały wpływ na koszty wykonania zamówienia przez Wykonawcę.
3. Zamawiający przewiduje możliwość dokonania zmiany terminu przewidzianego na zrealizowanie przedmiotu umowy w przypadku wydłużenia terminu realizacji grantów w projekcie „Cyberbezpieczny Samorząd”.
  4. Zamawiający przewiduje możliwość dokonania zmiany terminu przewidzianego na zrealizowanie przedmiotu zamówienia w przypadku konieczności spowolnienia lub wstrzymania wykonywania niniejszej umowy, ze względu na:
    - 1) wstrzymanie realizacji przedmiotu umowy przez Zamawiającego ze względu na czynniki, których Zamawiający nie mógł przewidzieć;
    - 2) zmianę zakresu zamówienia;
    - 3) zmiany terminu realizacji Umowy ze względu na przyczyny będące konsekwencją zaistnienia zdarzeń spowodowanych przez „siłę wyższą” (tj. zdarzenia nagle powstałe niezależnie od Stron Umowy, które są poza kontrolą Stron Umowy, na których czas trwania Strony nie mają jakiegokolwiek wpływu, a których zaistnienie uniemożliwia wypełnienie któregośkolwiek z zobowiązań wynikających z Umowy);
  5. Warunkiem dokonania zmian, o których mowa powyżej jest:
    - 1) zainicjowanie zmian przez Wykonawcę lub Zamawiającego,
    - 2) uzasadnienie zmiany,
    - 3) forma pisemna pod rygorem nieważności.
  6. Strony postanawiają, że w przypadku zmiany stawki podatku od towarów i usług – wynagrodzenie przewidziane niniejszą Umową ulegnie zmianie odpowiedniej do zmiany wysokości podatku od towarów i usług (ulegnie korekcie o wysokość zmiany podatku VAT), przy czym powyższa zmiana będzie miała zastosowanie wyłącznie w odniesieniu do wynagrodzenia objętego fakturami wystawionymi po dacie wejścia w życie zmiany przepisów prawa wprowadzających nowe stawki podatku od towarów i usług.
  7. Nie stanowi zmiany Umowy zmiana danych rejestrowych lub adresowych oraz ich danych kontaktowych.
  8. Wszystkie powyższe zapisy stanowią katalog zmian, na które Zamawiający może wyrazić zgodę. Nie stanowią jednocześnie zobowiązania do wyrażenia takiej zgody.

## § 12

### Ochrona i przetwarzanie danych osobowych

1. W trakcie realizacji umowy Zamawiający oraz Wykonawca, będą przekazywać dane osobowe niezbędne do realizacji zamówienia. Na warunkach określonych niniejszą umową strony będą przetwarzać dane osobowe, poprzez wspólne ustalenie celów i sposobów przetwarzania tych danych.



2. Przetwarzanie danych osobowych będzie wykonywane przez okres trwania umowy. Dane osobowe będą przetwarzane przez Strony wyłącznie w celu wykonania przedmiotu niniejszej umowy.
3. Przetwarzanie danych osobowych będzie dotyczyć następujących kategorii danych osobowych:
  - a) Ze strony Zamawiającego: dane pracowników do kontaktu.
  - b) Ze strony Wykonawcy: dane pracowników wykonujących przedmiot niniejszej umowy.
4. Przetwarzanie będzie obejmować dane zwykłe takie jak: imię i nazwisko, nr telefonu, adres e-mail, stanowisko, tytuł zawodowy, firmę adres i NIP pracodawcy, firmę adres i NIP prowadzonej działalności.
5. Strony nie będą przetwarzać danych osobowych szczególnej kategorii o których mowa w art. 9 ust. 1 RODO.
6. Zamawiający oświadcza, że jest administratorem danych, o których mowa w ust. 3a.
7. Wykonawca oświadcza, że jest administratorem danych, o których mowa w ust. 3b.
8. Po wykonaniu przedmiotu zamówienia, Strony usuwają / zwracają udostępnione przez drugą stronę dane osobowe oraz usuwają wszelkie istniejące ich kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
9. Strony zobowiązują się:
  - a) przetwarzać powierzone im dane osobowe zgodnie z niniejszą umową, Rozporządzeniem, ustawą o ochronie danych osobowych oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą,
  - b) do zabezpieczenia przetwarzanych danych, poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia,
  - c) dołożyć należytej staranności przy przetwarzaniu udostępnianych danych osobowych,
  - d) do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy,
  - e) zapewnić zachowanie w tajemnicy (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
10. Strony pomagają sobie w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia. Każda ze Stron niezwłocznie przekazuje żądanie osoby, której dane dotyczą, Administratorowi, który realizuje żądanie osoby.
11. Po stwierdzeniu naruszenia ochrony danych osobowych Strony bez zbędnej zwłoki zgłaszają je drugiemu administratorowi, nie później niż w ciągu 24 godzin od stwierdzenia naruszenia.
12. Strony, zgodnie z art. 28 ust. 3 pkt h Rozporządzenia mają prawo kontroli, czy środki zastosowane przy przetwarzaniu i zabezpieczeniu udostępnionych danych osobowych spełniają postanowienia umowy, w tym zlecenia jej wykonania audytorowi.
13. Strony będą realizować prawo kontroli w godzinach pracy Administratora informując o kontroli minimum 3 dni przed planowanym jej przeprowadzeniem.
14. Strony zobowiązują się do usunięcia uchybień stwierdzonych podczas kontroli w terminie nie dłuższym niż 7 dni.
15. Strony udostępnią na żądanie drugiego administratora wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

16. Strony przyjmują, że Wykonawca może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Zamawiającego.
17. Podwykonawca, winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Wykonawcę.
18. Wykonawca ponosi pełną odpowiedzialność wobec Zamawiającego za działanie podwykonawcy w zakresie obowiązku ochrony danych.
19. Strony zobowiązują się do niezwłocznego poinformowania współadministratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania danych osobowych określonych w umowie, o jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych.
20. Strony zobowiązują się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od współadministratora oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
21. Strony oświadczają, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.
22. W sprawach nieuregulowanych niniejszym paragrafem, zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.

#### **§ 10. Zachowanie poufności**

1. Strony umowy zobowiązują się do utrzymania w tajemnicy i nie przekazywania osobom trzecim, w tym także nieupoważnionym pracownikom, informacji i danych, które strony uzyskały w trakcie lub w związku z realizacją umowy, bez względu na sposób i formę ich utrwalenia lub przekazania, w szczególności w formie pisemnej, kserokopii, faksu i zapisu elektronicznego, o ile informacje takie nie są powszechnie znane, bądź obowiązek ich ujawnienia nie wynika z obowiązujących przepisów, orzeczeń sądowych lub decyzji odpowiednich władz.
2. Zasadą poufności nie jest objęty fakt zawarcia oraz warunki umowy.
3. Ujawnienie przez którąkolwiek ze stron informacji poufnej, z zastrzeżeniem przepisu ust. 1, wymagać będzie każdorazowo pisemnej zgody drugiej strony, chyba, że są to informacje publicznie dostępne, a ich ujawnienie nie nastąpiło w wyniku naruszenia postanowień niniejszej umowy.
4. Obowiązek zachowania poufności nałożony jest na strony umowy bezterminowo.
5. Każda ze stron niezwłocznie informuje drugą stronę o ujawnieniu informacji, organie, któremu informacje zostały ujawnione oraz zakresie ujawnienia.

#### **§ 13**

#### **Postanowienia końcowe**

1. Wykonawca nie ma prawa dokonywać cesji, przeniesienia bądź obciążenia swoich praw lub obowiązków wynikających z Umowy bez uprzedniej pisemnej zgody Zamawiającego, udzielonej na piśmie pod rygorem nieważności.
2. Wszelkie spory będą poddane pod rozstrzygnięcie sądu powszechnego właściwego dla siedziby Zamawiającego.
3. W sprawach nie uregulowanych zastosowanie mają przepisy Ustawy, ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny oraz inne mające związek z przedmiotową Umową.
4. Wszelkie zmiany Umowy, jej uzupełnienie lub oświadczenia z nią związane wymagają formy pisemnej pod rygorem nieważności.
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, jeden dla Wykonawcy, jeden dla Zamawiającego.
6. Integralną część Umowy stanowią następujące Załączniki:
  - 1) Specyfikacja Warunków Zamówienia.
  - 2) Oferta Wykonawcy.





**Załącznik Nr 3 do SWZ**  
**Wzór formularza ofertowego**  
(Znak postępowania: IN.271.2.3.2026.AK)

**A.DANE DOTYCZĄCE ZAMAWIAJĄCEGO.**

**Gmina Potok Górny** zwana dalej „Zamawiającym”

Potok Górny 116, 23-423 Potok Górny,

NIP: 918-19-89-917, REGON: 950369155,

nr telefonu +48 (84) 685 25 00,

Adres poczty elektronicznej: [sekretariat@potokgorny.com.pl](mailto:sekretariat@potokgorny.com.pl)

Strona internetowa Zamawiającego [URL]: <https://potokgorny.com.pl>

**B. DANE WYKONAWCY/WYKONAWCÓW.**

**1. Osoba upoważniona do reprezentacji Wykonawcy/-ów i podpisująca ofertę:**

.....

**2. Nazwa albo imię i nazwisko Wykonawcy<sup>1</sup>:**

.....

.....

Siedziba albo miejsce zamieszkania i adres Wykonawcy:

.....

NIP .....,

REGON.....

**3. Adres e-mail, na który w szczególnie uzasadnionych przypadkach uniemożliwiających komunikację Wykonawcy i Zamawiającego za pośrednictwem Platformy e-Zamówienia należy przekazywać korespondencję związaną z niniejszym postępowaniem:**

**e-mail:** .....

**4. Adres do korespondencji pisemnej, w sprawach, w których może ona być w tej formie prowadzona (jeżeli inny niż adres siedziby):**

.....

**5. Osoba odpowiedzialna za kontakty z Zamawiającym:**

.....

<sup>1</sup> Powielić tyle razy, ile to potrzebne

## C. OFEROWANY PRZEDMIOT ZAMÓWIENIA:

W związku z ogłoszeniem postępowania o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym na zadanie pn.

### „Zakup sprzętu IT wraz z oprogramowaniem w ramach projektu Zwiększenie cyberbezpieczeństwa Gminy Potok Górny”

#### W zakresie Części 1 Dostawa serwerów z oprogramowaniem

Oferuję/oferujemy\* wykonanie zamówienia zgodnie z zakresem prac zamieszczonym w opisie przedmiotu zamówienia zawartym w Zapytaniu ofertowym:

za łączną cenę oferty<sup>2</sup>:

brutto ..... zł

(słownie brutto:

.....zł).

netto..... zł

podatek (.....%)..... zł

w tym za:

Lp.	Nazwa	Ilość	Wartość netto za 1 szt. lub kpl.	Łączna wartość netto
1.	Zakup serwera z oprogramowaniem typ I	1 szt.		
2.	Zakup serwera z oprogramowaniem typ II	1 szt.		
3.	Zakup i wdrożenie rozwiązania Network Access Control	1 kpl.		
4.	Zakup oprogramowania do archiwizacji i kategoryzacji logów	1 kpl.		
5.	Zakup oprogramowania do inwentaryzacji i ochrony przed wyciekiem DLP	1 kpl.		
<b>Razem netto</b>				

<sup>2</sup> Należy wpisać łączną cenę wybranych do realizacji części zadania.



**W zakresie Części 2 Dostawa przełączników sieciowych, serwera NAS oraz UPS - a Oferuję/oferujemy\*** wykonanie zamówienia zgodnie z zakresem prac zamieszczonym w opisie przedmiotu zamówienia zawartym w Zapytaniu ofertowym:

za łączną cenę oferty<sup>3</sup>:

**brutto .....** zł

(słownie brutto:

.....zł).

**netto.....** zł

podatek (.....%)..... zł

w tym za:

Lp.	Nazwa	Ilość	Wartość netto za 1 szt. lub kpl.	Łączna wartość netto
1.	Zakup serwer NAS	2 kpl.		
2.	Zakup przełącznika sieciowego zarządzalnego	3 szt.		
3.	Zakup UPS	1 kpl.		
<b>Razem netto</b>				

#### D. OŚWIADCZENIE DOTYCZĄCE POSTANOWIEŃ TREŚCI SWZ.

- Oświadczam/y, że powyższa cena zawierają wszystkie koszty, jakie ponosi Zamawiający w przypadku wyboru niniejszej oferty na zasadach wynikających z umowy.
- Oświadczam/y, że zapoznałem/liśmy się z wymaganiami Zamawiającego, dotyczącymi przedmiotu zamówienia zamieszczonymi w SWZ wraz z załącznikami i nie wnoszę/wnosimy do nich żadnych zastrzeżeń.
- Oświadczam/y, że uważam/y się za związanych niniejszą ofertą przez okres wskazany w SWZ.
- Oświadczam/y, że zrealizuję/emy zamówienie zgodnie z SWZ i Projektem umowy.
- Oświadczam/y, że akceptuję/emy Regulamin Platformy e-Zamówienia dostępny na stronie <https://ezamowienia.gov.pl/pl/regulamin/#regulamin-serwisu> zawierający wiążące Wykonawcę informacje związane z korzystaniem z Platformy e-Zamówienia w szczególności opis sposobu składania/zmiany/wycofania oferty w niniejszym postępowaniu.
- Wadium zostało wniesione w formie  
.....  
Wadium należy zwrócić na nr konta: w banku:  
.....  
(jeżeli dotyczy)

- Oświadczam/y, że informacje i dokumenty zawarte w Ofercie na stronach

<sup>3</sup> Należy wpisać łączną cenę wybranych do realizacji części zadania.

od nr .....do nr ..... stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i zastrzegamy, że nie mogą być one udostępniane. Informacje i dokumenty zawarte na pozostałych stronach Oferty są jawne.

*(W przypadku utajnienia oferty Wykonawca zobowiązany jest wykazać, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa w szczególności określając, w jaki sposób zostały spełnione przesłanki, o których mowa w art. 11 pkt. 2 ustawy z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji).*

**8. Zobowiązujemy się dotrzymać wskazanego terminu realizacji zamówienia.**

**9. Pod groźbą odpowiedzialności karnej oświadczamy, iż wszystkie załączone do oferty dokumenty i złożone oświadczenia opisują stan faktyczny i prawny, aktualny na dzień składania ofert (art. 297 kk).**

**10. Składając niniejszą ofertę, zgodnie z art. 225 ust. 1 ustawy Pzp informuję, że wybór oferty<sup>4</sup>:**

- a) ☐ **nie będzie prowadzić** do powstania obowiązku podatkowego po stronie Zamawiającego, zgodnie z przepisami o podatku od towarów i usług, który miałby obowiązek rozliczyć,
- b) ☐ **będzie prowadzić** do powstania u Zamawiającego obowiązku podatkowego następujących towarów/usług:

.....	-
.....	zł netto
Nazwa towaru/usług	wartość bez kwoty podatku VAT

*\*Zgodnie z art. 225 ust. 2 ustawy Pzp, Wykonawca, składając ofertę, informuje Zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku. Należy zaznaczyć właściwe. Brak zaznaczenia będzie oznaczał, że wybór oferty Wykonawcy, nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego.*

**11. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO<sup>5</sup> wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu\***

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

## **E. ZOBOWIĄZANIE W PRZYPADKU PRYZNANIA ZAMÓWIENIA.**

- 1) Akceptuję proponowany przez Zamawiającego Projekt umowy, który zobowiązuję się podpisać w miejscu i terminie wskazanym przez Zamawiającego.
- 2) W przypadku wybrania mojej oferty, przed podpisaniem umowy wniosę zabezpieczenie należytego wykonania umowy w wysokości i na warunkach określonych w SWZ i Projekcie umowy.
- 3) Osobami uprawnionymi do merytorycznej współpracy i koordynacji w wykonywaniu zadania ze strony Wykonawcy są:

.....  
nr telefonu ....., e-mail: .....

<sup>4</sup> Należy odpowiednio zaznaczyć punkt a) albo b).

<sup>5</sup> rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).

## F. CZY WYKONAWCA JEST?

- ☐ mikroprzesiębiorstwem,
- ☐ małym przedsiębiorstwem,
- ☐ średnim przedsiębiorstwem,
- ☐ jednoosobową działalnością gospodarczą,
- ☐ osobą fizyczną nieprowadzącą działalności gospodarczej,
- ☐ inny rodzaj działalności.

*(zaznacz właściwe)*

## G. SPIS TREŚCI.

Integralną część oferty stanowią następujące dokumenty:

- 1) .....
- 2) .....
- 3) .....
- 4) .....
- 5) .....
- 6) .....
- 7) .....







## Załącznik Nr 4 do SWZ

### Wzór oświadczenia wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia składanego na podstawie art. 125 ust. 1 ustawy Pzp

(Znak postępowania: IN.271.2.3.2026.AK)

#### ZAMAWIAJĄCY:

Gmina Potok Górny zwana dalej „Zamawiającym”

Potok Górny 116, 23-423 Potok Górny,

NIP: 918-19-89-917, REGON: 950369155,

nr telefonu +48 (84) 685 25 00,

Adres poczty elektronicznej: [sekretariat@potokgorny.com.pl](mailto:sekretariat@potokgorny.com.pl)

Strona internetowa Zamawiającego [URL]: <https://potokgorny.com.pl>

#### WYKONAWCA:

.....  
.....  
.....

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

#### reprezentowany przez:

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

Na potrzeby postępowania o udzielenie zamówienia publicznego którego przedmiotem jest zadanie pn.: „Zakup sprzętu IT wraz z oprogramowaniem w ramach projektu Zwiększenie cyberbezpieczeństwa Gminy Potok Górny”, prowadzonego przez Gminę Potok Górny, **oświadczam, co następuje:**

#### **OŚWIADCZENIA DOTYCZĄCE PODSTAW WYKLUCZENIA:**

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy Pzp.
2. Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. .... ustawy Pzp (podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt. 1, 2 i 5 ustawy Prawo zamówień publicznych). Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjąłem następujące środki naprawcze i zapobiegawcze:  
.....
3. 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 (Dz. U. z 2025 poz. 175)<sup>1</sup>.

<sup>1</sup> Zgodnie z treścią 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, zwanej dalej „ustawą”, z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp 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 ustawy;

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, 655, 835, 2180 i 2185) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu

## OŚWIADCZENIE DOTYCZĄCE WARUNKÓW UDZIAŁU W POSTĘPOWANIU:

Oświadczam, że podmiot, w imieniu którego składane jest oświadczenie spełnia warunki udziału w postępowaniu określone przez Zamawiającego w rozdziale 6 Specyfikacji Warunków Zamówienia w zakresie warunku wskazanego w:

☐ pkt. 6.1.4, ppkt. 1),

☐ pkt. 6.1.4, ppkt. 2)

## INFORMACJA W ZWIĄZKU Z POLEGANIEM NA ZDOLNOŚCIACH LUB SYTUACJI PODMIOTÓW UDOSTĘPNIAJĄCYCH ZASOBY:

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez Zamawiającego w rozdziale 6 Specyfikacji Warunków Zamówienia w zakresie warunku wskazanego w:

☐ pkt. 6.1.4, ppkt. 1),

☐ pkt. 6.1.4, ppkt. 2)

polegam na zdolnościach lub sytuacji następującego/ych podmiotu/ów udostępniających zasoby:

.....  
(wskazać nazwę/y podmiotu/ów)

w następującym zakresie:

.....  
(określić odpowiedni zakres udostępnianych zasobów dla wskazanego podmiotu).

## 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.

## INFORMACJA DOTYCZĄCA DOSTĘPU DO PODMIOTOWYCH ŚRODKÓW DOWODOWYCH:

Wskazuję następujące podmiotowe środki dowodowe, które można uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, oraz dane umożliwiające dostęp do tych środków:

.....  
(wskazać podmiotowy środek dowodowy, adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji).





**Załącznik Nr 5 do SWZ**  
**Wzór oświadczenia podmiotu udostępniającego zasoby składanego**  
**na podstawie art. 125 ust. 1 ustawy Pzp**  
(Znak postępowania: IN.271.2.2.2026.AK)

**ZAMAWIAJĄCY:**

**Gmina Potok Górny** zwana dalej „Zamawiającym”

Potok Górny 116, 23-423 Potok Górny,

NIP: 918-19-89-917, REGON: 950369155,

nr telefonu +48 (84) 685 25 00,

Adres poczty elektronicznej: [sekretariat@potokgorny.com.pl](mailto:sekretariat@potokgorny.com.pl)

Strona internetowa Zamawiającego [URL]: <https://potokgorny.com.pl>

**PODMIOT UDOSTĘPNIAJĄCY ZASOBY:**

.....  
.....  
.....

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

**reprezentowany przez:**

.....  
.....

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Na potrzeby postępowania o udzielenie zamówienia publicznego którego przedmiotem jest zadanie pn.: „Zakup sprzętu IT wraz z oprogramowaniem w ramach projektu Zwiększenie cyberbezpieczeństwa Gminy Potok Górny”, prowadzonego przez Gminę Potok Górny, **oświadczam, co następuje:**

**OŚWIADCZENIA DOTYCZĄCE PODSTAW WYKLUCZENIA:**

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy Pzp.
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 (Dz. U. z 2025 poz.175)<sup>1</sup>.

<sup>1</sup> Zgodnie z treścią 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, zwanej dalej „ustawą”, z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp 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 ustawy;  
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, 655, 835, 2180 i 2185) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;  
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 oraz z 2022 r. poz. 1488), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy.

**OŚWIADCZENIE DOTYCZĄCE WARUNKÓW UDZIAŁU W POSTĘPOWANIU:**

Oświadczam, że podmiot, w imieniu którego składane jest oświadczenie spełnia warunki udziału w postępowaniu określone przez Zamawiającego w rozdziale 6 Specyfikacji Warunków Zamówienia w zakresie warunku wskazanego w:

☐ pkt. 6.1.4, ppkt. 1),☐ pkt. 6.1.4, ppkt. 2)

w następującym zakresie:

.....  
.....

**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.

**INFORMACJA DOTYCZĄCA DOSTĘPU DO PODMIOTOWYCH ŚRODKÓW DOWODOWYCH:**

Wskazuję następujące podmiotowe środki dowodowe, które można uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, oraz dane umożliwiające dostęp do tych środków:

.....

*(wskazać podmiotowy środek dowodowy, adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji).*

**Załącznik Nr 6 do SWZ**  
**Wzór oświadczenia Wykonawców wspólnie ubiegających się o udzielenie zamówienia**  
(Znak postępowania: IN.271.2.3.2026.AK)

**ZAMAWIAJACY:**

**Gmina Potok Górny** zwana dalej „Zamawiającym”

Potok Górny 116, 23-423 Potok Górny,

NIP: 918-19-89-917, REGON: 950369155,

nr telefonu +48 (84) 685 25 00,

Adres poczty elektronicznej: [sekretariat@potokgorny.com.pl](mailto:sekretariat@potokgorny.com.pl)

Strona internetowa Zamawiającego [URL]: <https://potokgorny.com.pl>

**PODMIOTY W IMIENIU KTÓRYCH SKŁADANE JEST OŚWIADCZENIE:**

.....

.....

.....

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

.....

.....

.....

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

**reprezentowane przez:**

.....

.....

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

**Oświadczenie składane na podstawie art. 117 ust. 4 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t. j. Dz. U. z 2024 r. poz. 1320 ze zm.) -  
dalej: ustawa Pzp**

Na potrzeby postępowania o udzielenie zamówienia publicznego którego przedmiotem jest robota budowlana na zadaniu inwestycyjnym pn. „Sporządzenie planu ogólnego Gminy Potok Górny”, prowadzonego przez Gminę Potok Górny, działając jako pełnomocnik podmiotów, w imieniu których składane jest oświadczenie oświadczam, że:

**Wykonawca:**

.....

Wykona następujący zakres świadczenia wynikającego z umowy o zamówienie publiczne:

.....

.....

**Wykonawca:**

.....

Wykona następujący zakres świadczenia wynikającego z umowy o zamówienie publiczne:



.....

.....

**UWAGA:**

**\*W przypadku, gdy ofertę składa spółka cywilna, a pełen zakres prac wykonają wspólnicy wspólnie w ramach umowy spółki oświadczenie powinno potwierdzać ten fakt.**

**Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą.**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska



Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

## Załącznik Nr 7 do SWZ Wzór wykazu dostaw (Znak postępowania: IN.271.2.3.2026.AK)

### ZAMAWIAJACY:

Gmina Potok Górny zwana dalej „Zamawiającym”

Potok Górny 116, 23-423 Potok Górny,

NIP: 918-19-89-917, REGON: 950369155,

nr telefonu +48 (84) 685 25 00,

Adres poczty elektronicznej: [sekretariat@potokgorny.com.pl](mailto:sekretariat@potokgorny.com.pl)

Strona internetowa Zamawiającego [URL]: <https://potokgorny.com.pl>

### WYKONAWCA:

.....

.....

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

reprezentowany przez:

.....

.....

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

### Wykaz dostaw wykonanych/wykonywanych wykonanych w okresie ostatnich 3 lat przed upływem terminu składania ofert

Na potrzeby postępowania o udzielenie zamówienia publicznego, którego przedmiotem jest dostawa w ramach zadania pn. „Zakup sprzętu IT wraz z oprogramowaniem w ramach projektu Zwiększenie cyberbezpieczeństwa Gminy Potok Górny”, prowadzonego przez Gminę Potok Górny, przedkładam wykaz zamówień zgodnie zapisami pkt. 6.1.4 SWZ wraz z podaniem ich przedmiotu, wartości, daty wykonania oraz określeniem podmiotów, na rzecz których roboty zostały wykonane:

w zakresie części:

☐ Część 1: „Dostawa serwerów z oprogramowaniem”.

☐ Część 2: „Dostawa przełączników sieciowych, serwera NAS oraz UPS - a”

Lp.	Rodzaj zrealizowanych dostaw (podanie nazwy i zakresu realizacji z opisem pozwalającym na ocenę spełniania warunku udziału w postępowaniu)	Zamawiający (nazwa podmiotu, na rzecz którego roboty te zostały wykonane)	Daty wykonania zamówienia		Wartość dostawy w zł (brutto)
			Data rozpoczęcia [dd/mm/rrrr]	Data zakończenia [dd/mm/rrrr]	
1.					
2.					

oraz

załączam dowody określające czy dostawy te zostały wykonane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego usługi zostały wykonane, a jeżeli Wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – inne odpowiednie dokumenty.



**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA****Opis charakterystyki zaoferowanego sprzętu informatycznego i oprogramowania****„Zakup sprzętu IT wraz z oprogramowaniem w ramach projektu Zwiększenie cyberbezpieczeństwa Gminy Potok Górny”**

Dostawa fabrycznie nowego sprzętu do Urzędu Gminy w Potoku Górnym, 23-423 Potok Górny 116 o wskazanych poniżej lub równoważnych parametrach i funkcjach technicznych nie gorszych niż wskazane.

**W ofercie należy podać nazwę producenta, typ, model, oferowanego sprzętu umożliwiającą jednoznaczną identyfikację oferowanej konfiguracji.**

Nie dopuszcza się modyfikacji na drodze Producent-Zamawiający (np. modyfikacji lub wymiany jakiegokolwiek komponentu sprzętowego).

Zakres zadania obejmuje w szczególności

Lp.	Nazwa	Ilość
<b>Część 1 Dostawa serwerów z oprogramowaniem</b>		
1.	Zakup serwera z oprogramowaniem typ I	1 szt.
2.	Zakup serwera z oprogramowaniem typ II	1 szt.
3.	Zakup i wdrożenie rozwiązania Network Access Control	1 kpl.
4.	Zakup oprogramowania do archiwizacji i kategoryzacji logów	1 kpl.
5.	Zakup oprogramowania do inwentaryzacji i ochrony przed wyciekiem DLP	1 kpl.
<b>Część 2 Dostawa przełączników sieciowych, serwera NAS oraz UPS - a</b>		
6.	Zakup serwer NAS	2 szt.
7.	Zakup przełącznika sieciowego zarządzalnego	3 szt.
8.	Zakup UPS	1 kpl.

**Wymagania ogólne.**

1. Dostarczony sprzęt i oprogramowanie muszą być wolne od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt i oprogramowanie muszą być fabrycznie nowe (tzn. wyprodukowane nie wcześniej, niż na 12 miesięcy przed ich dostarczeniem), muszą pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu i oprogramowania.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale”, „end-of-support”, „end-of-life” producenta lub innych listach prowadzonych przez producentów produktów świadczących o tym, że produkt został wycofany ze sprzedaży, wsparcie dla niego zostało zakończone lub producent zaprzestaje wydawania aktualizacji, poprawek bezpieczeństwa czy też napraw dla produktu.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek

zewnętrznych przejściówek czy konwerterów. Niedopuszczalna jest realizacja tylko części funkcji bądź wymaganych standardów zamiast innych określonych jako minimalne w niniejszym dokumencie. Wszystkie wymagania minimalne muszą zostać zapewnione przez dostarczane produkty bez konieczności zakupu żadnych dodatkowych elementów przez Zamawiającego, chyba że z niniejszego dokumentu wynika inaczej.

5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do wskazanej przez Zamawiającego lokalizacji.
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzeń do działania, pozwalające na rozpoczęcie pracy oraz dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.
8. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
9. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
10. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
11. Dla dostaw sprzętu informatycznego z oprogramowaniem Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania (w tym systemu operacyjnego) nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania (faktury, rachunki) w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
12. Dla dostaw oprogramowania Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania, nieużywanego oraz nigdy wcześniej nieaktywowanego oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania posiadającego fizyczny nośnik naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

W poniższych tabelach przedstawiono minimalne wymagania w zakresie specyfikacji technicznej poszczególnych pozycji.

## 1 ZAKUP SERWERA Z OPROGRAMOWANIEM TYP I- 1 KPL.

L.p	Parametr	Charakterystyka (wymagania minimalne)	
1.	Obudowa	<ul style="list-style-type: none"> <li>- Obudowa Rack o wysokości 1U.</li> <li>- 8 wnęk na dyski 2.5".</li> <li>- Możliwość instalacji dysków SAS/SATA/M.2 – Fabryczna blokada demontowania dysków twardych zamykana na klucz lub za pomocą zamka lub innego podobnego zabezpieczenia.</li> <li>- LCD na froncie obudowy lub diody LED informujące o stanie komponentów np. CPU, RAM, SSD, zasilanie.</li> </ul>	<b>Producent:</b>  <b>Model wersja:</b>
2.	Płyta główna	<ul style="list-style-type: none"> <li>- Płyta główna z możliwością zainstalowania jednego procesora.</li> <li>- Obsługa procesorów 144 rdzeniowych.</li> <li>- Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.</li> <li>- Na płycie głównej powinny znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.</li> <li>- Płyta główna powinna obsługiwać do 4TB pamięci RAM.</li> </ul>	SPEŁNIA TAK /NIE
3.	Procesor	<ul style="list-style-type: none"> <li>- Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych.</li> <li>- Zainstalowany jeden procesor min. 12-rdzeniowy, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 140 w teście SPECspeed@2017_fp_base, dostępnym na stronie <a href="http://www.spec.org">www.spec.org</a> dla konfiguracji jednoprocessorowej oferowanego serwera</li> </ul>	SPEŁNIA TAK /NIE
4.	RAM	<ul style="list-style-type: none"> <li>- 64 GB DDR5 RDIMM.</li> <li>- Pamięć RAM musi wspierać wczesne wykrywanie błędów poprawialnych (CE) w pamięci i przeprowadzanie operacji izolacji. Pamięć musi wspierać typowe technologie ochrony m.in. ECC, Address/Command Parity, PPR, Write Data CRC Protection, ADC-SR, ADDDC-MR, SDDC.</li> </ul>	SPEŁNIA TAK /NIE
5.	Kontroler RAID	<ul style="list-style-type: none"> <li>- Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID 0, 1, 10, 5, 6, 60.</li> </ul>	SPEŁNIA TAK /NIE
6.	Dyski twarde	<ul style="list-style-type: none"> <li>- Zainstalowane min. 3 dyski 2,5-calowe: <ul style="list-style-type: none"> <li>o 2 x 1,9 TB minimum (HDD, 10000 obr./min, SAS 12 Gb/s, 2.5", Hot-Plug)</li> <li>o 1 x 480 GB minimum (SSD, SATA 6 Gb/s, 2.5", Hot-Plug)</li> </ul> </li> <li>- Możliwość zainstalowania dwóch dysków M.2 SSD o pojemności 480GB Hot-Plug z możliwością konfiguracji RAID 1.</li> </ul>	SPEŁNIA TAK /NIE
7.	Gniazda PCIe	<ul style="list-style-type: none"> <li>- 2x PCIe 4.0 x16</li> </ul>	SPEŁNIA TAK /NIE
8.	Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> <li>- Min. 2 interfejsy sieciowe 1GBe BASE-T</li> <li>- Min. 2 interfejsy sieciowe SFP+ 10GbE</li> </ul>	SPEŁNIA TAK /NIE
9.	Wbudowane porty oraz wskaźniki	<ul style="list-style-type: none"> <li>- 3 porty USB w tym min: <ul style="list-style-type: none"> <li>o 1 port USB 3.1,</li> <li>o 1 port USB z przodu obudowy</li> <li>o 1 port USB 2.0 Type-C</li> </ul> </li> <li>- 1 port VGA</li> </ul>	
10.	Video	<ul style="list-style-type: none"> <li>- Zintegrowana karta graficzna osiągająca rozdzielczość 1920x1200</li> </ul>	SPEŁNIA TAK /NIE
11.	Wentylatory	<ul style="list-style-type: none"> <li>- Redundantne</li> </ul>	SPEŁNIA TAK /NIE
12.	Zasilacze	<ul style="list-style-type: none"> <li>- Minimum dwa redundantne zasilacze każdy o mocy zapewniającej prawidłową pracę serwera, moc minimum 800W</li> </ul>	SPEŁNIA TAK /NIE
13.	Elementy montażowe	<ul style="list-style-type: none"> <li>- Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych</li> </ul>	SPEŁNIA TAK /NIE



14.	<b>Bezpieczeństwo</b>	<ul style="list-style-type: none"> <li>- Moduł TPM 2.0</li> <li>- Secure boot</li> <li>- Ochrona przed atakami. Urządzenie musi udostępniać minimalną wymaganą liczbę portów usług sieciowych. Domyślnie, zbędne usługi muszą być wyłączone, porty usług sieciowych do debugowania i diagnozy muszą być wyłączone podczas normalnej pracy serwera.</li> </ul>	SPEŁNIA TAK /NIE
15.	<b>BIOS</b>	<ul style="list-style-type: none"> <li>- Oferowany serwer musi być wyposażony w BIOS zapewniający następujące funkcjonalności: <ul style="list-style-type: none"> <li>o Inicjalizacja sprzętu: BIOS musi wspierać pełne testowanie i uruchamianie kluczowych komponentów serwera, takich jak procesory, pamięć RAM, dyski twarde oraz interfejsy sieciowe.</li> <li>o Zarządzanie konfiguracją systemu: BIOS musi umożliwiać konfigurację ustawień systemowych, w tym kolejności bootowania, konfiguracji RAID oraz ustawień zasilania.</li> <li>o Bezpieczeństwo systemu: BIOS musi wspierać funkcję Secure Boot, chroniącą przed uruchamianiem nieautoryzowanego oprogramowania. Musi również posiadać opcję zabezpieczenia hasłem dostępu.</li> </ul> </li> <li>- Aktualizacje oprogramowania: BIOS musi umożliwiać aktualizację firmware'u oraz zapewniać wsparcie dla aktualizacji zdalnych.</li> </ul>	SPEŁNIA TAK /NIE
16.	<b>Bezpieczeństwo</b>	<ul style="list-style-type: none"> <li>- Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania.</li> <li>- Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</li> <li>- BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła</li> <li>- Moduł TPM 2.0</li> <li>- Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera</li> <li>- Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem</li> <li>- Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155.</li> </ul>	SPEŁNIA TAK /NIE
17.	<b>Karta Zarządzania</b>	<ul style="list-style-type: none"> <li>- Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające:</li> <li>- zdalny dostęp do graficznego interfejsu Web karty zarządzającej</li> <li>- szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika</li> <li>- możliwość podmontowania zdalnych wirtualnych napędów</li> <li>- wirtualną konsolę z dostępem do myszy, klawiatury</li> <li>- wsparcie dla IPv6</li> <li>- wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH</li> <li>- integracja z Active Directory</li> <li>- możliwość obsługi przez trzech administratorów jednocześnie</li> <li>- Wsparcie dla automatycznej rejestracji DNS</li> <li>- wsparcie dla LLDP</li> <li>- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej</li> <li>- możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy.</li> <li>- Monitorowanie zużycia dysków SSD</li> <li>- Automatyczne update firmware dla wszystkich komponentów</li> </ul>	SPEŁNIA TAK /NIE

## Załącznik Nr 8

		<p>serwera</p> <ul style="list-style-type: none"> <li>- Możliwość przywrócenia poprzednich wersji firmware</li> <li>- Możliwość eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, konfiguracji kontrolera RAID) serwera do pliku XML lub JSON lub innego</li> <li>- Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych</li> <li>- Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.</li> <li>- kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania</li> </ul>	
18.	Oprogramowanie do zarządzania	<ul style="list-style-type: none"> <li>- Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:</li> <li>- integracja z Active Directory</li> <li>- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta</li> <li>- Wsparcie dla protokołów SNMP, IPMI, Linux SSH,</li> <li>- Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram</li> <li>- Szczegółowy opis wykrytych systemów oraz ich komponentów</li> <li>- Możliwość eksportu raportu do CSV, HTML, XLS, PDF</li> <li>- Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.</li> <li>- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach</li> <li>- Szybki podgląd stanu środowiska</li> <li>- Podsumowanie stanu dla każdego urządzenia</li> <li>- Szczegółowy status urządzenia/elementu/komponentu</li> <li>- Generowanie alertów przy zmianie stanu urządzenia.</li> <li>- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń</li> <li>- Możliwość przejęcia zdalnego pulpitu</li> <li>- Możliwość podmontowania wirtualnego napędu</li> <li>- Kreator umożliwiający dostosowanie akcji dla wybranych alertów</li> <li>- Przesyłanie alertów „as-is” do innych konsol firm trzecich</li> <li>- Możliwość definiowania ról administratorów</li> <li>- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów</li> <li>- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)</li> <li>- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta</li> <li>- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.</li> <li>- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.</li> <li>- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.</li> <li>- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.</li> <li>- Zdalne uruchamianie diagnostyki serwera.</li> <li>- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.</li> </ul>	SPEŁNIA TAK /NIE
19.	Oprogramowanie do monitorowania	<ul style="list-style-type: none"> <li>- Oparta na chmurze aplikacja Producenta oferowanego urządzenia,</li> </ul>	SPEŁNIA TAK /NIE

		<p>która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</p> <ul style="list-style-type: none"> <li>- Monitoring:</li> <li>- ilość podłączonych oraz rozłączonych systemów</li> <li>- stan podłączonych urządzeń</li> <li>- informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów</li> <li>- Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia</li> <li>- informacje o statusie gwarancji dla poszczególnych urządzeń</li> <li>- informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń</li> <li>- Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych</li> <li>- Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących.</li> <li>- Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.</li> <li>- Monitoring parametrów serwerów z informacją o minimum:</li> <li>- Obciążeniu procesora</li> <li>- Zużyciu pamięci RAM</li> <li>- Temperaturze procesorów</li> <li>- Zmianach w fizycznej konfiguracji serwera</li> <li>- Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.</li> <li>- Aktualizacja firmware</li> <li>- możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania</li> <li>- Raporty</li> <li>- Możliwość generowania raportów dla serwerów zawierających informację o:</li> <li>- Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej</li> <li>- Średnim obciążeniu: procesorów, pamięci RAM, IO,</li> <li>- Generowanie raportów do plików CSV i PDF</li> <li>- Cyberbezpieczeństwo</li> <li>- Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.</li> <li>- Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce.</li> <li>- Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.</li> <li>- Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.</li> </ul>	
20.	Certyfikaty	<ul style="list-style-type: none"> <li>- Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent serwera opracował, wdrożył i certyfikował system zarządzania jakością;</li> <li>- Certyfikat ISO 50001 lub Certyfikat ISO 14001 lub inny równoważny dokument poświadczający, że producent serwera posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność;</li> </ul>	



		<ul style="list-style-type: none"> <li>- Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany serwer spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE;</li> <li>- Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych.</li> <li>- Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.</li> </ul>	
21.	<b>System operacyjny/dodatkowe oprogramowanie</b>	<ul style="list-style-type: none"> <li>- Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego klasy Microsoft Windows Serwer Standard w najnowszej dostępnej wersji oferowanej przez producenta oprogramowania umożliwiającego uruchomienie serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.</li> <li>- Warunki równoważności dla dostawy oprogramowania Microsoft Windows Serwer Standard w najnowszej wersji oferowanej przez producenta oprogramowania: <ul style="list-style-type: none"> <li>a) Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji oraz dostępu do serwerowego systemu operacyjnego.</li> <li>b) Możliwość wykorzystywania 248 procesorów wirtualnych oraz 24TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.</li> <li>c) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.</li> <li>d) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.</li> <li>e) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.</li> <li>f) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.</li> <li>g) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.</li> <li>h) Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;</li> <li>i) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</li> <li>j) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.</li> <li>k) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.</li> <li>l) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.</li> <li>m) Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</li> </ul> </li> </ul>	<p><b>Producent:</b></p> <p><b>Model wersja:</b></p> <p><b>SPEŁNIA TAK /NIE</b></p>

		<p>n) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.</p> <p>o) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.</p> <p>p) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play).</p> <p>q) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</p> <p>r) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).</p> <p>s) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.</p> <p>t) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</p> <p>u) Co najmniej 10 lat wsparcia długoterminowego.</p> <p>v) Wsparcie protokołu SMB za pośrednictwem rozwiązania QUIC.</p>	
22.	Licencje dostępne	25 Licencji dostępowych uprawniających na korzystanie z usług serwera. Licencja „na użytkownika”	SPEŁNIA TAK /NIE
23.	Dokumentacja użytkownika	<ul style="list-style-type: none"> <li>- Zamawiający wymaga dokumentacji w języku polskim lub angielskim oraz dostęp do oprogramowania wymaganego do poprawnego funkcjonowania serwera.</li> <li>- Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</li> <li>- Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia</li> </ul>	SPEŁNIA TAK /NIE
24.	Warunki serwisu i gwarancji	<ul style="list-style-type: none"> <li>- Gwarancja: min. 24 miesiące gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dysków Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii w języku polskim poprzez ogólnopolską linię telefoniczną producenta oraz dedykowany portal techniczny producenta, dla obu kanałów w trybie ciągłym, tj. niezależnie od pory dnia, dni roboczych i dni wolnych od pracy</li> <li>- Zamawiający wymaga przynajmniej dwóch podstawowych form kontaktu serwisowego tj. całodobowej infolinii oraz formularza online.</li> <li>- Oferowane wsparcie musi być świadczone w języku polskim bezpośrednio przez Producenta.</li> <li>- Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.</li> <li>- Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</li> <li>- Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.</li> <li>- w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego</li> </ul>	SPEŁNIA TAK /NIE

25.	Wsparcie serwisowe	W przypadku jeżeli serwis gwarancyjny urządzeń nie będzie realizowany bezpośrednio przez producenta urządzenia, wówczas firma serwisująca musi posiadać certyfikat ISO 9001 oraz ISO 27001 lub inny równoważny dokument poświadczający, że usługi serwisu świadczone będą zgodnie z zasadami wynikającymi z tych norm oraz firma serwisująca musi posiadać autoryzacje producenta urządzeń.	SPEŁNIA TAK /NIE
-----	--------------------	---	------------------

## 2 ZAKUP SERWERA Z OPROGRAMOWANIEM TYP II- 1 KPL.

L.p	Parametr	Charakterystyka (wymagania minimalne)	
1.	Obudowa	<ul style="list-style-type: none"> <li>- Obudowa Rack o wysokości 1U.</li> <li>- 8 wnęk na dyski 2.5".</li> <li>- Możliwość instalacji dysków SAS/SATA/M.2 – Fabryczna blokada demontowania dysków twardych zamykana na klucz lub za pomocą zamka lub innego podobnego zabezpieczenia.</li> <li>- LCD na froncie obudowy lub diody LED informujące o stanie komponentów np. CPU, RAM, SSD, zasilanie.</li> </ul>	<b>Producent:</b>  <b>Model wersja:</b>
2.	Płyta główna	<ul style="list-style-type: none"> <li>- Płyta główna z możliwością zainstalowania jednego procesora.</li> <li>- Obsługa procesorów 144 rdzeniowych.</li> <li>- Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.</li> <li>- Na płycie głównej powinny znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.</li> <li>- Płyta główna powinna obsługiwać do 4TB pamięci RAM.</li> </ul>	SPEŁNIA TAK /NIE
3.	Procesor	<ul style="list-style-type: none"> <li>- Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych.</li> <li>- Zainstalowany jeden procesor min. 8-rdzeniowy, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 80 w teście SPECspeed@2017_fp_base, dostępnym na stronie <a href="http://www.spec.org">www.spec.org</a> dla konfiguracji jednoprocessorowej oferowanego serwera – wyniki testu załączyć do oferty.</li> </ul>	SPEŁNIA TAK /NIE
4.	RAM	<ul style="list-style-type: none"> <li>- 32 GB DDR5 RDIMM.</li> <li>- Pamięć RAM musi wspierać wczesne wykrywanie błędów poprawialnych (CE) w pamięci i przeprowadzanie operacji izolacji. Pamięć musi wspierać typowe technologie ochrony m.in. ECC, Address/Command Parity, PPR, Write Data CRC Protection, ADC-SR, ADDDC-MR, SDDC.</li> </ul>	SPEŁNIA TAK /NIE
5.	Kontroler RAID	<ul style="list-style-type: none"> <li>- Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID 0, 1, 10, 5, 6, 60.</li> </ul>	SPEŁNIA TAK /NIE
6.	Dyski twarde	<ul style="list-style-type: none"> <li>- Zainstalowane min. 3 dyski 2,5-calowe: <ul style="list-style-type: none"> <li>o 2 x 1,9 TB minimum (HDD, 10000 obr./min, SAS 12 Gb/s, 2.5", Hot-Plug)</li> <li>o 1 x 480 GB minimum (SSD, SATA 6 Gb/s, 2.5", Hot-Plug)</li> </ul> </li> <li>- Możliwość zainstalowania dwóch dysków M.2 SSD o pojemności 480GB Hot-Plug z możliwością konfiguracji RAID 1.</li> </ul>	SPEŁNIA TAK /NIE
7.	Gniazda PCIe	<ul style="list-style-type: none"> <li>- 2x PCIe 4.0 x16</li> </ul>	SPEŁNIA TAK /NIE
8.	Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> <li>- Min. 2 interfejsy sieciowe 1GBe BASE-T</li> <li>- Min. 2 interfejsy sieciowe SFP+ 10GbE</li> </ul>	SPEŁNIA TAK /NIE
9.	Wbudowane porty oraz wskaźniki	<ul style="list-style-type: none"> <li>- 3 porty USB w tym min: <ul style="list-style-type: none"> <li>o 1 port USB 3.1,</li> <li>o 1 port USB z przodu obudowy</li> <li>o 1 port USB 2.0 Type-C</li> </ul> </li> <li>- 1 port VGA</li> </ul>	SPEŁNIA TAK /NIE
10.	Video	<ul style="list-style-type: none"> <li>- Zintegrowana karta graficzna osiągająca rozdzielczość 1920x1200</li> </ul>	SPEŁNIA



## Załącznik Nr 8

			TAK /NIE
11.	<b>Wentylatory</b>	- Redundantne	SPEŁNIA TAK /NIE
12.	<b>Zasilacze</b>	- Minimum dwa redundantne zasilacze każdy o mocy zapewniającej prawidłową pracę serwera, moc minimum 700W	SPEŁNIA TAK /NIE
13.	<b>Elementy montażowe</b>	- Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych	SPEŁNIA TAK /NIE
14.	<b>Bezpieczeństwo</b>	- Moduł TPM 2.0 - Secure boot - Ochrona przed atakami. Urządzenie musi udostępniać minimalną wymaganą liczbę portów usług sieciowych. Domyślnie, zbędne usługi muszą być wyłączone, porty usług sieciowych do debugowania i diagnozy muszą być wyłączone podczas normalnej pracy serwera.	SPEŁNIA TAK /NIE
15.	<b>BIOS</b>	- Oferowany serwer musi być wyposażony w BIOS zapewniający następujące funkcjonalności: <ul style="list-style-type: none"> <li>o Inicjalizacja sprzętu: BIOS musi wspierać pełne testowanie i uruchamianie kluczowych komponentów serwera, takich jak procesory, pamięć RAM, dyski twarde oraz interfejsy sieciowe.</li> <li>o Zarządzanie konfiguracją systemu: BIOS musi umożliwiać konfigurację ustawień systemowych, w tym kolejności bootowania, konfiguracji RAID oraz ustawień zasilania.</li> <li>o Bezpieczeństwo systemu: BIOS musi wspierać funkcję Secure Boot, chroniącą przed uruchamianiem nieautoryzowanego oprogramowania. Musi również posiadać opcję zabezpieczenia hasłem dostępu.</li> </ul> - Aktualizacje oprogramowania: BIOS musi umożliwiać aktualizację firmware'u oraz zapewniać wsparcie dla aktualizacji zdalnych.	SPEŁNIA TAK /NIE
16.	<b>Bezpieczeństwo</b>	- Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. - Możliwość wyłączenia w BIOS funkcji przycisku zasilania. - BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła - Moduł TPM 2.0 - Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera - Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem - Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155.	SPEŁNIA TAK /NIE
17.	<b>Karta Zarządzania</b>	- Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej - szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika - możliwość podmontowania zdalnych wirtualnych napędów - wirtualną konsolę z dostępem do myszy, klawiatury - wsparcie dla IPv6 - wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH - integracja z Active Directory - możliwość obsługi przez trzech administratorów jednocześnie - Wsparcie dla automatycznej rejestracji DNS	SPEŁNIA TAK /NIE

		<ul style="list-style-type: none"> <li>- wsparcie dla LLDP</li> <li>- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej</li> <li>- możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy.</li> <li>- Monitorowanie zużycia dysków SSD</li> <li>- Automatyczne update firmware dla wszystkich komponentów serwera</li> <li>- Możliwość przywrócenia poprzednich wersji firmware</li> <li>- Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, konfiguracji kontrolera RAID) serwera do pliku XML lub JSON lub innego</li> <li>- Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych</li> <li>- Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.</li> <li>- kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania</li> </ul>	
18.	Oprogramowanie do zarządzania	<ul style="list-style-type: none"> <li>- Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:</li> <li>- integracja z Active Directory</li> <li>- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta</li> <li>- Wsparcie dla protokołów SNMP, IPMI, Linux SSH,</li> <li>- Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram</li> <li>- Szczegółowy opis wykrytych systemów oraz ich komponentów</li> <li>- Możliwość eksportu raportu do CSV, HTML, XLS, PDF</li> <li>- Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.</li> <li>- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach</li> <li>- Szybki podgląd stanu środowiska</li> <li>- Podsumowanie stanu dla każdego urządzenia</li> <li>- Szczegółowy status urządzenia/elementu/komponentu</li> <li>- Generowanie alertów przy zmianie stanu urządzenia.</li> <li>- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń</li> <li>- Możliwość przejęcia zdalnego pulpitu</li> <li>- Możliwość podmontowania wirtualnego napędu</li> <li>- Kreator umożliwiający dostosowanie akcji dla wybranych alertów</li> <li>- Przesyłanie alertów „as-is” do innych konsol firm trzecich</li> <li>- Możliwość definiowania ról administratorów</li> <li>- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów</li> <li>- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)</li> <li>- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta</li> <li>- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.</li> <li>- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.</li> <li>- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami</li> </ul>	SPEŁNIA TAK /NIE

		<p>sieciowymi (MAC, WWN, IQN) między urządzeniami.</p> <ul style="list-style-type: none"> <li>- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.</li> <li>- Zdalne uruchamianie diagnostyki serwera.</li> <li>- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.</li> </ul>	
19.	<b>Oprogramowanie do monitorowania</b>	<ul style="list-style-type: none"> <li>- Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</li> <li>- Monitoring:</li> <li>- ilość podłączonych oraz rozłączonych systemów</li> <li>- stan podłączonych urządzeń</li> <li>- informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów</li> <li>- Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia</li> <li>- informacje o statusie gwarancji dla poszczególnych urządzeń</li> <li>- informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń</li> <li>- Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych</li> <li>- Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących.</li> <li>- Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.</li> <li>- Monitoring parametrów serwerów z informacją o minimum:</li> <li>- Obciążeniu procesora</li> <li>- Zużyciu pamięci RAM</li> <li>- Temperaturze procesorów</li> <li>- Zmianach w fizycznej konfiguracji serwera</li> <li>- Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliiach.</li> <li>- Aktualizacja firmware</li> <li>- możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania</li> <li>- Raporty</li> <li>- Możliwość generowania raportów dla serwerów zawierających informację o:</li> <li>- Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej</li> <li>- Średnim obciążeniu: procesorów, pamięci RAM, IO,</li> <li>- Generowanie raportów do plików CSV i PDF</li> <li>- Cyberbezpieczeństwo</li> <li>- Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.</li> <li>- Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce.</li> <li>- Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.</li> <li>- Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.</li> </ul>	SPĘŁNIA TAK /NIE



## Załącznik Nr 8

20.	Certyfikaty	<ul style="list-style-type: none"> <li>- Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent serwera opracował, wdrożył i certyfikował system zarządzania jakością;</li> <li>- Certyfikat ISO 50001 lub Certyfikat ISO 14001 lub inny równoważny dokument poświadczający, że producent serwera posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność;</li> <li>- Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany serwer spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE;</li> <li>- Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. - Wykonawca złoży dokument potwierdzający spełnianie wymogu</li> <li>- Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.</li> </ul>	SPEŁNIA TAK /NIE
21.	System operacyjny/dodatkové oprogramowanie	<ul style="list-style-type: none"> <li>- Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego klasy Microsoft Windows Server Standard w najnowszej dostępnej wersji oferowanej przez producenta oprogramowania umożliwiającego uruchomienie serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.</li> <li>- Warunki równoważności dla dostawy oprogramowania Microsoft Windows Server Standard w najnowszej wersji oferowanej przez producenta oprogramowania: <ul style="list-style-type: none"> <li>w) Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji oraz dostępu do serwerowego systemu operacyjnego.</li> <li>x) Możliwość wykorzystywania 248 procesorów wirtualnych oraz 24TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.</li> <li>y) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.</li> <li>z) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.</li> <li>aa) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.</li> <li>bb) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.</li> <li>cc) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.</li> <li>dd) Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;</li> <li>ee) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</li> <li>ff) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się</li> </ul> </li> </ul>	<b>Producent:</b>  <b>Model wersja:</b>  SPEŁNIA TAK /NIE

		<p>bezpieczeństwem informacji.</p> <p>gg) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.</p> <p>hh) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.</p> <p>ii) Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</p> <p>jj) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.</p> <p>kk) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.</p> <p>ll) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&amp;Play).</p> <p>mm) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.</p> <p>nn) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).</p> <p>oo) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.</p> <p>pp) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</p> <p>qq) Co najmniej 10 lat wsparcia długoterminowego.</p> <p>rr) Wsparcie protokołu SMB za pośrednictwem rozwiązania QUIC.</p>	
22.	<b>Licencje dostępne</b>	10 Licencji dostępowych uprawniających na korzystanie z usług serwera. Licencja na użytkownika	SPEŁNIA TAK /NIE
23.	<b>Dokumentacja użytkownika</b>	<ul style="list-style-type: none"> <li>- Zamawiający wymaga dokumentacji w języku polskim lub angielskim oraz dostęp do oprogramowania wymaganego do poprawnego funkcjonowania serwera.</li> <li>- Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</li> <li>- Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia</li> </ul>	SPEŁNIA TAK /NIE
24.	<b>Warunki serwisu i gwarancji</b>	<ul style="list-style-type: none"> <li>- Gwarancja: min. 24 miesiące gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dysków Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii w języku polskim poprzez ogólnopolską linię telefoniczną producenta oraz dedykowany portal techniczny producenta, dla obu kanałów w trybie ciągłym, tj. niezależnie od pory dnia, dni roboczych i dni wolnych od pracy</li> <li>- Zamawiający wymaga przynajmniej dwóch podstawowych form kontaktu serwisowego tj. całodobowej infolinii oraz formularza online.</li> <li>- Oferowane wsparcie musi być świadczone w języku polskim bezpośrednio przez Producenta.</li> <li>- Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.</li> <li>- Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</li> <li>- Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi</li> </ul>	SPEŁNIA TAK /NIE

		<p>serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.</p> <ul style="list-style-type: none"> <li>- w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego</li> </ul>	
25.	<b>Wsparcie serwisowe</b>	W przypadku jeżeli serwis gwarancyjny urządzeń nie będzie realizowany bezpośrednio przez producenta urządzenia, wówczas firma serwisująca musi posiadać certyfikat ISO 9001 oraz ISO 27001 lub inny równoważny dokument poświadczający, że usługi serwisu świadczone będą zgodnie z zasadami wynikającymi z tych norm oraz firma serwisująca musi posiadać autoryzację producenta urządzeń.	SPEŁNIA TAK /NIE

### 3 ZAKUP I WDROŻENIE ROZWIĄZANIA NETWORK ACCESS CONTROL- 110 IP

L.P	Parametr	Charakterystyka (wymagania minimalne)	
1.	Dane producenta /model	Producent oferowanego rozwiązania /model i wersja modelu	<b>Producent:</b>  <b>Model wersja:</b>  SPEŁNIA TAK /NIE
2.	Opis funkcjonalności rozwiązania	<p>Wymagane jest dostarczenie rozwiązania typu NAC (Network Access Control), służącego do monitorowania sieci lokalnych w celu uwidocznienia pracujących w nich urządzeń oraz wykrywania nowych urządzeń pojawiających się w sieci, w czasie rzeczywistym. Rozwiązanie musi raportować aktualny stan każdego urządzenia, z uwzględnieniem takich atrybutów, jak adres MAC, adres IP, nazwa hosta, system operacyjny, itp., pozyskując te informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.).</p> <p>Rozwiązanie ma za zadanie zapewnić, aby tylko urządzenia, których aktualny stan spełnia zdefiniowaną przez administratora politykę bezpieczeństwa, mogły bez ograniczeń ze strony NAC pracować w sieci lokalnej. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenia, których aktualny stan nie spełnia danych warunków polityki bezpieczeństwa (np. nowe, po raz pierwszy pojawiające się urządzenie lub stacja robocza z wyłączonym oprogramowaniem antywirusowym). Mechanizm kwarantanny powinien umożliwiać całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym, jak również blokowanie częściowe, w zakresie definiowanym przez administratora (przez wskazanie adresów IP, z którymi urządzenie może się komunikować). Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej.</p> <p>Rozwiązanie musi posiadać funkcjonalność typu Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów.</p>	SPEŁNIA TAK /NIE
3.	Wymagania ogólne rozwiązania NAC	<p>1.Ma zapewnić widoczność i monitorowanie wszystkich urządzeń pracujących w sieci lokalnej oraz powiadamiać o nowych urządzeniach pojawiających się w sieci.</p> <p>2.Musi zapewniać automatyczne blokowanie komunikacji sieciowej między nowym, niezauważanym urządzeniem a zaufanymi, zarządzanymi urządzeniami pracującymi w sieci.</p>	SPEŁNIA TAK /NIE



		<p>3. Musi umożliwiać sprawdzanie statusu aktualizacji oprogramowania antywirusowego i poprawek systemowych na zarządzanych stacjach roboczych Windows i w przypadku niespełniania określonych wymagań, automatycznie ograniczać tym stacjom roboczym możliwość pracy w sieci.</p> <p>4. Musi umożliwiać odbieranie komunikatów bezpieczeństwa z innych systemów bezpieczeństwa (np. firewalla) i automatyczne blokowanie na tej podstawie wskazanych urządzeń w sieci.</p> <p>5. Musi mieć funkcję wykrywania faktu skanowania urządzeń i portów wykonywanego przez urządzenie w sieci lokalnej i automatycznie blokować takie urządzenie, aby zapobiegać potencjalnemu szerzeniu się malware.</p> <p>6. Stosowany mechanizm blokowania musi wykorzystywać protokół ARP i działać całkowicie niezależnie od innych elementów infrastruktury sieciowej.</p> <p>7. Rozwiązanie musi działać bezagentowo, bez konieczności instalowania jakichkolwiek agentów na urządzeniach w sieci oraz bez konieczności dokonywania zmian w infrastrukturze sieciowej.</p> <p>8. Rozwiązanie musi umożliwiać wysyłanie alertów do administratora za pomocą e-maila oraz SMS</p> <p>9. Rozwiązanie musi być zarządzane przez interfejs webowy, obsługiwany przeglądarką internetową</p> <p>10. <b>Wymaga się, aby rozwiązanie było dostarczone w postaci maszyny wirtualnej na platformę Vmware lub Hyper-V. System musi pozwalać na monitorowanie co najmniej 5 sieci VLAN.</b></p> <p>11. <b>Wymaga się, aby rozwiązanie było licencjonowane w modelu licencji wieczystej i dostarczone z licencją pozwalającą na monitorowanie 110 urządzeń wraz ze wsparciem technicznym na okres do końca czerwca 2026</b></p>	
4.	Wymagania szczegółowe – monitorowanie podsieci	<p>1. Rozwiązanie musi w czasie rzeczywistym raportować widoczność wszystkich urządzeń pracujących w monitorowanych podsieciach.</p> <p>2. Rozwiązanie musi wykrywać nowe nieznanne urządzenie, dołączające się do sieci LAN lub WLAN, w czasie nie dłuższym, niż 5 sekund oraz wysłać powiadomienie mailowe do administratora</p> <p>3. Rozwiązanie musi wykrywać przypadki skanowania urządzeń i portów w monitorowanych podsieciach i blokować urządzenie inicjujące takie skanowanie</p> <p>4. Rozwiązanie musi posiadać funkcję pułapki sieciowej (honeypot), symulującą w każdej monitorowanej podsieci standardowe usługi sieciowe, co najmniej: ssh, telnet, ftp i smb. Rozwiązanie musi rejestrować każdą próbę zalogowania się do takiej symulowanej usługi, zapisując użytą nazwę użytkownika, hasło użytkownika i źródłowy MAC/IP.</p> <p>5. Rozwiązanie musi określać aktualny stan każdego urządzenia, pozyskując informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.) oraz odświeżać te informacje cyklicznie. Musi być możliwość wykorzystania pozyskanych informacji do definiowania polityk bezpieczeństwa.</p> <p>6. Rozwiązanie musi chronić przed podszywaniem się pod adres MAC (MAC spoofing), umożliwiając zdefiniowanie „odcisku palca” (fingerprint) dla każdego zaufanego urządzenia. Odcisk palca musi być kombinacją co najmniej: adresu MAC, adresu IP, nazwy hosta, nazwy systemu operacyjnego, otwartych portów TCP. Jeśli przeprowadzana cyklicznie weryfikacja odcisku palca wykaze jego zmianę, urządzenie powinno zostać zablokowane.</p> <p>7. Rozwiązanie musi obsługiwać VLANy, tj. umożliwiać monitorowanie przez jeden fizyczny interfejs sieciowy wielu podsieci, zdefiniowanych jako VLANy</p>	SPEŁNIA TAK /NIE
5.	Wymagania szczegółowe – polityka	<p>1. Rozwiązanie musi umożliwiać definiowanie polityki bezpieczeństwa, czyli określenie przez administratora, jakie warunki musi spełniać aktualny stan urządzenia, aby uzyskało ono określony dostęp do sieci.</p>	SPEŁNIA TAK /NIE

	bezpieczeństwa	<p>2. W definiowaniu polityki bezpieczeństwa musi być możliwość wykorzystania informacji o aktualnym stanie urządzenia, pozyskanych bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.), poprzez integrację z tymi systemami.</p> <p>3. Polityka bezpieczeństwa musi umożliwiać przypisanie do urządzenia jednego z trzech trybów dostępu do sieci:</p> <ul style="list-style-type: none"> <li>a. pełny dostęp</li> <li>b. blokowanie (całkowity brak dostępu)</li> <li>c. ograniczony dostęp</li> </ul> <p>4. Zakres ograniczonego dostępu powinien być definiowany przez administratora, np. w postaci list ACL, określających, do których adresów IP i portów urządzenie ma dostęp. Musi być możliwość zdefiniowania wielu różnych zakresów ograniczonego dostępu.</p> <p>5. Rozwiązanie powinno automatycznie sprawdzać, które warunki polityki bezpieczeństwa spełnia urządzenie i na tej podstawie przypisywać do urządzenia właściwy zakres dostępu.</p> <p>6. Zakres dostępu, wynikający ze spełnienia przez urządzenie danych warunków polityki bezpieczeństwa powinien być egzekwowany przez mechanizm kwarantanny.</p> <p>7. Musi być możliwość łatwego, manualnego tworzenia białej listy adresów MAC, czyli listy urządzeń mogących bez żadnych ograniczeń ze strony NAC pracować w sieci.</p>	
6.	Wymagania szczegółowe – mechanizm kwarantanny	<p>1. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenie, aby wyegzekwować ograniczenia dostępu do sieci, wynikające z polityki bezpieczeństwa</p> <p>2. Mechanizm kwarantanny powinien umożliwiać:</p> <ul style="list-style-type: none"> <li>a. całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym,</li> <li>b. częściowe blokowanie komunikacji urządzenia z otoczeniem sieciowym, w zakresie definiowanym przez administratora przez wskazanie adresów IP i portów, z którymi urządzenie może się komunikować</li> </ul> <p>3. Mechanizm kwarantanny powinien blokować komunikację urządzenia w czasie nie dłuższym niż 5 sekund od zaistnienia warunku, powodującego nałożenie kwarantanny</p> <p>4. Dla urządzeń zaufanych, czyli w polityce bezpieczeństwa spełniających kryteria pełnego dostępu do sieci, rozwiązanie nie powinno w żaden sposób przekierowywać ani blokować komunikacji wychodzącej z tych urządzeń</p> <p>5. Kwarantanna powinna być zdejmowana z urządzenia automatycznie, gdy spełni ono kryteria polityki bezpieczeństwa, pozwalające na pełny dostęp</p> <p>6. Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej, musi być niezależny od stosowanych w sieci przełączników, zarządzalnych bądź niezarządzalnych</p> <p>7. Awaria rozwiązania nie może powodować blokady komunikacji w sieci, tj. w przypadku awarii rozwiązania wszystkie urządzenia mają mieć pełny dostęp do sieci</p> <p>8. Rozwiązanie musi umożliwiać włączenie i wyłączenie mechanizmu kwarantanny (blokowania komunikacji) w każdej monitorowanej podsieci osobno</p>	SPEŁNIA TAK /NIE
7.	Wymagania szczegółowe – integracja z systemami zewnętrznymi	<p>1. Rozwiązanie musi umieć sprawdzić, czy urządzenia z systemem Windows są dołączone do domeny AD</p> <p>2. Rozwiązanie powinno umożliwiać sprawdzanie statusu oprogramowania antywirusowego, poprawek systemowych i firewalla bezpośrednio na zarządzanych stacjach roboczych Windows w domenie AD, w sposób bezagentowy, przy użyciu WMI.</p> <p>3. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym poprawkami Windows i sprawdzanie statusu zainstalowanych poprawek na zarządzanych urządzeniach z systemem Windows. Wymagana jest możliwość integracji co najmniej z systemami:</p>	SPEŁNIA TAK /NIE

		<p>Microsoft WSUS.</p> <p>4. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym agentami antywirusowymi i sprawdzanie statusu agentów AV zainstalowanych na zarządzanych urządzeniach (co najmniej, czy agent jest zainstalowany, aktywny i ma aktualne sygnatury wirusów). Wymagana jest możliwość integracji co najmniej z systemami: Bitdefender, Carbon Black, CrowdStrike, Cybereason, Eset, FireEye, McAfee, SentinelOne, Sophos, Symantec, TrendMicro, Webroot.</p> <p>5. Rozwiązanie musi umożliwiać wykorzystanie pozyskanych informacji, wymienionych w poprzedzających punktach 1-4, do definiowania polityki bezpieczeństwa.</p> <p>6. Rozwiązanie musi umieć odbierać alerty przysyłane za pomocą e-mail lub syslog z innych urządzeń bezpieczeństwa (np. firewalla) i na podstawie zawartych w nich informacji blokować wskazane podejrzaną urządzenie</p>	
8.	Wymagania szczegółowe – rejestracja urządzeń zewnętrznych: pracowników, gości i konsultantów (Captive Portal)	<p>1. Rozwiązanie musi posiadać wbudowaną funkcję Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów. NAC musi przekierowywać ruch HTTP/S od nieznanego urządzenia do tego portalu.</p> <p>2. Captive Portal musi umożliwiać pracownikom rejestrowanie urządzeń prywatnych (BYOD) i wnioskowanie o dostęp do sieci w ograniczonym zakresie, zdefiniowanym przez administratora.</p> <p>3. Przy rejestracji przez pracowników ich prywatnych urządzeń, Captive Portal powinien umożliwiać użycie ich kont Active Directory</p> <p>4. Powinna istnieć możliwość ograniczenia ilości i rodzaju rejestrowanych przez pracownika prywatnych urządzeń</p> <p>5. Powinna być możliwość przypisania ograniczonego dostępu dla zarejestrowanych urządzeń prywatnych</p> <p>6. Captive Portal musi umożliwiać osobom niebędącym pracownikami (gościom lub konsultantom) wnioskowanie o ograniczony dostęp do sieci</p> <p>7. W przypadku rejestracji urządzeń gości powinna być możliwość rejestracji samodzielnie przez gościa oraz przez uprawnionego pracownika firmy</p> <p>8. Zarejestrowane urządzenia gości powinny automatycznie tracić przydzielony dostęp po upływie zdefiniowanego czasu</p> <p>9. Powinna istnieć możliwość ograniczenia ilości urządzeń rejestrowanych przez gościa</p> <p>10. Dla zarejestrowanych urządzeń gości powinna być możliwość ograniczenia, w jakich przedziałach czasu i z jakich podsieci będą one miały dostęp do sieci</p> <p>11. Dla urządzeń gości powinna być możliwość przypisania dostępu ograniczonego tylko do dostępu do internetu</p> <p>12. Dla urządzeń konsultantów powinna być możliwość przypisania dostępu ograniczonego do wybranych zasobów lokalnych</p> <p>13. Rozwiązanie musi umożliwiać zatwierdzenie dostępu dla zarejestrowanego urządzenia gościa i konsultanta drogą mailową. Osoba zatwierdzająca powinna otrzymać z systemu e-mail z wnioskiem o dostęp i udzielić go, odpowiadając na maila lub klikając przygotowany link w treści maila.</p> <p>14. Rozwiązanie musi przechowywać historyczne raporty dostępu do sieci użytkowników typu gość i konsultant</p> <p>15. Wygląd Captive Portal musi być edytowalny w zakresie co najmniej zmiany firmowego logo i kolorów oraz informacji, jakie we wniosku rejestracyjnym musi podać gość lub konsultant</p>	SPEŁNIA TAK /NIE
9.	Pozostałe wymagania	<p>1. Rozwiązanie powinno oferować uwierzytelnianie administratora za pomocą dodatkowego faktora, oprócz hasła (2FA).</p> <p>2. Rozwiązanie powinno oferować możliwość zainstalowania opcjonalnego agenta na zarządzanych stacjach roboczych (wymagane wsparcie dla Windows, Linux i MacOS), który przesyła do serwera zarządzającego NAC szczegółowe informacje na temat stacji roboczej, umożliwiając definiowanie na bazie tych informacji precyzyjnych polityk</p>	SPEŁNIA TAK /NIE



## Załącznik Nr 8

		<p>bezpieczeństwa.</p> <p>3. Rozwiązanie nie powinno pogarszać wydajności pracy przełączników i routerów, nie może wymagać współpracy z przełącznikami przez port mirroring czy port spanning.</p> <p>4. Rozwiązanie nie powinno pogarszać wydajność łącz WAN</p> <p>5. Rozwiązanie nie powinno pogarszać wydajności pracy monitorowanych urządzeń w sieci</p>	
10.	Usługi	<p>Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego, w wymienionym poniżej zakresie, przeprowadzoną przez wykwalifikowanego inżyniera, certyfikowanego przez producenta rozwiązania w siedzibie Zamawiającego:</p> <ul style="list-style-type: none"> <li>- instalacja i konfiguracja rozwiązania w maszynie wirtualnej na platformie Zamawiającego</li> <li>- szkolenie dla administratora rozwiązania</li> <li>- wsparcie w języku polskim w trybie 8x5 w dni robocze</li> <li>- kwartalny przegląd konfiguracji rozwiązania</li> </ul> <p>Wymaga się, aby dostawca przedstawił:</p> <ul style="list-style-type: none"> <li>- <b>oświadczenie Producenta lub Autoryzowanego Dystrybutora Producenta o posiadaniu przez dostawcę kwalifikacji technicznych, niezbędnych do wykonania wdrożenia oferowanego rozwiązania i szkolenia</b></li> <li>- <b>osobowy certyfikat inżynierski pracownika, która będzie wykonywał wdrożenie,</b></li> </ul>	SPEŁNIA TAK /NIE
11.	Wsparcie	<p>Wymaga się, aby dostawca zaoferował usługę zdalnego wsparcia w zakresie reagowania na raportowane przez NAC zdarzenia, przez okres minimum do końca czerwca 2026</p> <ul style="list-style-type: none"> <li>- w trybie ciągłym 24/7, z czasem reakcji 4 godziny, w zakresie:</li> <li>- alertów wysyłanych przez NAC</li> <li>- bieżąca analiza raportowanych zdarzeń pod kątem istniejącego zagrożenia bezpieczeństwa sieci</li> <li>- merytoryczne wsparcie w procesie reagowania na raportowane przez NAC zagrożenia</li> </ul>	SPEŁNIA TAK /NIE

#### 4 OPROGRAMOWANIE DO ARCHIWIZACJI I KATEGORYZACJI LOGÓW.

L.P.	Parametr	Wymagania minimalne	
1.	Dane producenta	Producent oferowanego rozwiązania	Producent
2.	Charakterystyka rozwiązania	<ol style="list-style-type: none"> <li>1. Rozwiązanie musi odbierać wiadomości Syslog</li> <li>2. Rozwiązanie musi odbierać wiadomości Trap SNMP w wersji v1,v2, v3</li> <li>3. Rozwiązanie musi nasłuchiwać Windows Event Log</li> <li>4. Rozwiązanie musi posiadać graficzny interfejs użytkownika w przeglądarce internetowej</li> <li>5. Rozwiązanie musi mieć możliwość powiadamiania użytkowników drogą emailową na bazie otrzymanych zdarzeń</li> <li>6. Rozwiązanie musi mieć możliwość uruchamiania zewnętrznych skryptów</li> <li>7. Rozwiązanie musi mieć możliwość przesyłania dalej zebranych wiadomości do innych systemów w formatach Syslog oraz Trap SNMP w wersji v1, v2, v3</li> <li>8. Rozwiązanie musi mieć możliwość eksportu zdarzeń do formatu .csv</li> <li>9. Rozwiązanie powinno umożliwiać zarządzanie politykami retencji danych zdarzeń</li> <li>10. Rozwiązanie musi wspierać standard IPv4 i IPv6</li> <li>11. Rozwiązanie musi wspierać przesył danych na poziomie powyżej 2 000 000 zdarzeń na godzinę</li> <li>12. Rozwiązanie musi być licencjonowanie w sposób nieograniczający ilości</li> </ol>	<p>Spełnia</p> <p>TAK/NIE</p>

		podłączonych urządzeń przesyłających informacje 13. Rozwiązanie powinno integrować się ze Splunk 14. Rozwiązanie powinno integrować się z rozwiązaniami typu SIEM 15. Rozwiązanie musi mieć możliwość instalacji na systemach Microsoft Windows Server 2019, 2022, 2025 oraz Microsoft Windows 10, 11.	
3.	Licencjonowanie	Licencja wieczysta na oprogramowanie, wsparcie techniczne przez okres minimum do końca czerwca 2026	Spełnia TAK/NIE
4.	Usługi	Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego, : - instalacja i konfiguracja rozwiązania na platformie Zamawiającego - szkolenie dla administratora rozwiązania - wsparcie w języku polskim w trybie 8x5 w dni robocze	Spełnia TAK/NIE

## 5 OPROGRAMOWANIE DO INWENTARYZACJI I OCHRONY PRZED WYCIEKIEM DLP - 25 LICENCJI.

LP	Parametr	Wymagania minimalne	PRODUCENT  NAZWA I WERSJA OPROGRAMOWANIA
	Dane producenta	Przedmiotem zamówienia jest dostawa licencji wieczystej i wdrożenie oprogramowania do zarządzania bezpieczeństwem IT umożliwiającego szereg funkcji podnoszących cyberbezpieczeństwo	
1.	<b>Architektura / budowa</b>	<ol style="list-style-type: none"> <li>System musi umożliwić i stabilną obsługę co najmniej 25 Klientów jednocześnie.</li> <li>Architektura / budowa: <ol style="list-style-type: none"> <li>Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.</li> <li>Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).</li> <li>Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.</li> <li>Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.</li> </ol> </li> <li>Konfiguracja Architektury: <ol style="list-style-type: none"> <li>Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.</li> <li>System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.</li> </ol> </li> </ol>	SPEŁNIA TAK /NIE
2.	<b>Wymagania systemowe</b>	<ol style="list-style-type: none"> <li>Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera).</li> <li>Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2016/2019/2022/2025 Windows 7/8/8.1/10/11, Linux</li> <li>Wsparcie poniższych przeglądarek internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera, Chrome, FireFox</li> <li>Serwer musi działać na systemach 64 bitowych: Windows Server 2019/2022/2025, Windows 7/8/8.1/10/11.</li> <li>Baza danych musi działać na silniku bezpłatnym System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare i innych.</li> </ol>	SPEŁNIA TAK /NIE

## Załącznik Nr 8

3.	<b>Interfejs</b>	<ol style="list-style-type: none"> <li>System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory,</li> <li>System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL</li> <li>System zapewnia integrację z modelem LLM.</li> </ol>	SPEŁNIA TAK /NIE
4.	<b>Funkcjonalności systemu zarządzania infrastrukturą IT</b>	<ol style="list-style-type: none"> <li>System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkownika.</li> <li>Konsola administracyjna musi być w języku polskim i oferować interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie).</li> <li>W konsoli powinna istnieć funkcja filtrowania danych</li> <li>Konsola musi umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.</li> <li>Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników.</li> <li>Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników.</li> <li>System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania.</li> <li>System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office.</li> <li>System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich połączeń.</li> <li>System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.</li> <li>System musi umożliwiać inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.</li> </ol> <p><b>Ochrona danych (DLP)</b></p> <ol style="list-style-type: none"> <li>System musi monitorować i zapobiegać wyciekom danych (DLP) poprzez bieżące (w czasie rzeczywistym) monitorowanie działań użytkowników wg ściśle zdefiniowanych polityk bezpieczeństwa</li> </ol>	SPEŁNIA TAK /NIE



		<p>oraz reguł ich opisujących.</p> <ol style="list-style-type: none"> <li>13. System musi zapewniać automatyczne uruchamianie ochrony zasobów w czasie rzeczywistym zgodnie ze zdefiniowanymi politykami.</li> <li>14. System musi zapewniać ciągłą ochronę danych niezależnie od położenia komputera (w sieci lokalnej, sieci VPN, poza siecią).</li> <li>15. System musi mieć możliwość konfiguracji i instalacji dowolnej ilości reguł dla dowolnych polityk DLP.</li> <li>16. System musi mieć możliwość czasowej dezaktywacji danej reguły bez jej usuwania i utraty konfiguracji.</li> <li>17. System musi w pełni wspierać następujące polityki ochrony danych: Zdefiniowanie schematu, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione. Wyświetlanie komunikatu na komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne z poziomu konsoli administracyjnej z wykorzystaniem edytora (możliwość utworzenia tabeli, dołączenia obrazu, wstawienia linku).</li> <li>18. System musi umożliwiać monitorowanie danych przesyłanych za pomocą poczty e-mail oraz blokowanie przesyłania plików określonych typów. (E-MAIL)</li> <li>19. System musi monitorować dane przesyłane do chmury oraz blokować synchronizację plików określonych typów z wybraną chmurą.</li> <li>20. System musi umożliwiać monitorowanie i blokowanie operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach.</li> <li>21. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami.</li> <li>22. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie.</li> <li>23. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.</li> <li>24. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.</li> <li>25. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.</li> <li>26. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o</li> </ol>	
--	--	---	--

		<p>zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.</p> <p>27. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.</p> <p>28. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie.</p> <p>29. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.</p> <p>30. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikiem a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania.</p> <p>31. System musi posiadać możliwość eksportu / importu treści.</p> <p>32. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku. System powinien pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.</p> <p>33. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron do klasyfikacji i kontroli treści.</p> <p>34. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.</p> <p>35. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.</p> <p>36. System musi umożliwiać monitorowanie komunikatów Syslog.</p> <p>37. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.</p> <p>38. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizację danych i filtrami do zarządzania informacjami.</p> <p>39. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.</p> <p>40. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o</p>	
--	--	---	--

		<p>oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.</p> <p>41. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostępnienia w panelu pracownika.</p> <p>42. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.</p> <p>43. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki.</p> <p>44. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co predefiniowane powiadomienia oraz możliwość ich personalizacji.</p> <p>45. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymagc silnych haseł, obsługa wieloskładnikowego uwierzytelniania i posiadać mechanizmy szyfrowania danych.</p> <p>46. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami.</p> <p>47. System musi zapewniać kompleksowe wsparcie użytkowników poprzez helpdesk, interfejs do zgłaszania i zarządzania problemami, możliwość edycji i nadawania priorytetów zgłoszeniom oraz konfigurację powiadomień odpowiednich.</p>	
5.	<b>Wsparcie i pomoc</b>	<p>1. Pomoc techniczna musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.</p> <p>2. Zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.</p> <p>3. Czas trwania usługi SLA wynosi od dnia zakupu lecz nie może przekroczyć terminu 30 czerwca 2026</p>	SPEŁNIA TAK /NIE
6.	<b>Wdrożenie</b>	<p>1. Komunikacja musi odbywać się w języku polskim,</p> <p>2. Wdrożenie obejmuje pełną konfigurację wszystkich modułów niezbędnych do uruchomienia systemu</p> <p>3. Wdrożenie zakończone jest szkoleniem z obsługi oprogramowania</p>	SPEŁNIA TAK /NIE



## 6 SERWER NAS - 2 sztuki

L.p	Parametr	Charakterystyka (wymagania minimalne)	Producent
1.	Przeznaczenie	Urządzenie do przechowywania danych – system NAS	<b>Model i wersja</b>
2.	Procesor	Wielordzeniowy procesor osiągający wynik minimum 4,5 tys. punktów w teście PassMark.	SPEŁNIA TAK /NIE
3.	Obudowa	Typu rack o wysokości maksymalnie 2U z zestawem szyn przesuwnych umożliwiających montaż w szafie rack.	SPEŁNIA TAK /NIE
4.	Pamięć RAM	Minimum 16GB DDR4 ECC tego samego producenta co serwer.	SPEŁNIA TAK /NIE
5.	Interfejsy sieciowe	Minimum 4 porty 1GbE RJ-45. Obsługa agregacji łącz.	SPEŁNIA TAK /NIE
6.	Ilość obsługiwanych dysków	Minimum 8 dysków o maksymalnej pojemności nie mniejszej niż 18TB każdy, po podłączeniu modułów rozszerzających minimum 12 dysków.	SPEŁNIA TAK /NIE
7.	Zainstalowane dyski	8 dysków o pojemności 12 TB każdy zgodnych z listą kompatybilności oferowanego rozwiązania oraz charakteryzujących się następującymi parametrami: - prędkość obrotowa: minimum 7200 RPM, - gwarancja: minimum 24 miesiące, - MTBF: minimum 1 200 000 h, - możliwość aktualizacji oprogramowania dysków bezpośrednio z interfejsu systemu operacyjnego serwera NAS.	SPEŁNIA TAK /NIE
8.	Gniazda rozszerzeń	Minimum 1 slot PCIe Gen3	SPEŁNIA TAK /NIE
9.	Wskaźniki LED	Status, dyski, zasilanie, LAN	SPEŁNIA TAK /NIE
10.	Obsługa RAID	RAID 0, 1, 5, 6, 10. Obsługa dysków zapasowych typu hot spare.	SPEŁNIA TAK /NIE
11.	Funkcje RAID	Możliwość zwiększania pojemności poprzez wymianę dysków na większe. Migracja poziomu RAID w trybie online dla minimum RAID 1 i RAID 5.	SPEŁNIA TAK /NIE
12.	Szyfrowanie	Możliwość szyfrowania wybranych udziałów sieciowych.	SPEŁNIA TAK /NIE
13.	Protokoły	SMB, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP	SPEŁNIA TAK /NIE
14.	Usługi	1. Serwer VPN, Serwer pocztowy, Stacja monitoringu, Windows ACL, Integracja z Windows Active Directory, Firewall, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Usługa DDNS, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki, możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów. 2. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 7 lub nowszym według harmonogramu z centralnej konsoli zarządzania dostępnej lokalnie oraz zdalnie, z możliwością przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Bez ograniczenia liczby podłączanych komputerów do systemu kopii zapasowej. 3. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klastr obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora.	SPEŁNIA TAK /NIE
15.	Zarządzanie dyskami	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów,	SPEŁNIA TAK /NIE

## Załącznik Nr 8

16.	System plików	Dyski wewnętrzne: BTRFS, EXT4 Dyski zewnętrzne: FAT, NTFS, EXT3, EXT4, HFS+.	SPEŁNIA TAK /NIE
17.	Język GUI	Polski	SPEŁNIA TAK /NIE
18.	Certyfikaty	CE,	SPEŁNIA TAK /NIE
19.	Szyfrowanie	Mechanizm szyfrowania sprzętowego.	SPEŁNIA TAK /NIE
20.	Zasilanie	Pojedynczy zasilacz o mocy maksymalnie 350W.	SPEŁNIA TAK /NIE
21.	Opcje software'owe	1. zarządzanie NAS poprzez minimum przeglądarkę internetową, GUI oparte o HTML5; 2. NAS musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączenia NAS; 3. NAS musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową; 4. NAS musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów NAS, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – nie jest wymagane dostarczenie licencji dla tej funkcjonalności; 5. Serwer plików, Serwer FTP, WebDav, Serwer WEB, Serwer kopii zapasowych, Serwer Monitoringu,	SPEŁNIA TAK /NIE
22.	Konfiguracja, zarządzanie	1. komunikacja z wbudowanym oprogramowaniem zarządzającym NAS musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW jak również w trybie tekstowym. 2. musi być możliwe zdalne zarządzanie NAS z wykorzystaniem standardowej przeglądarki internetowej (np. Edge, Opera, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora	SPEŁNIA TAK /NIE
23.	Gwarancja i serwis	1. 2 lata gwarancji producenta NAS w trybie onsite z gwarantowanym czasem skutecznej naprawy najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw. tryb Next Business Day); 2. Gwarancja producenta na dyski: 2 lat 3. uszkodzone dyski zawierające dane pozostają własnością Zamawiającego i nie będą zwracane do serwisu producenta NAS, w ich miejsce w ramach 2-letniego okresu gwarancji zostaną dostarczone nowe; 4. serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego,	SPEŁNIA TAK /NIE
24.	Jakość produktu i sposobu jego wykonania	Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany NAS spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta NAS lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych.	SPEŁNIA TAK /NIE

## 7 PRZEŁĄCZNIKI ZARZĄDZALNE – 3 szt

L.P	Parametr	Charakterystyka (wymagania minimalne)	
1.	<b>CECHY ZARZĄDZANIA</b>		
2.	Typ przełącznika	Zarządzany	<b>Producent</b>

## Załącznik Nr 8

			Model i wersja
3.	Przełącznik wielowarstwowy	L2/L3	SPEŁNIA TAK /NIE
4.	Obsługa jakości serwisu (QoS)	Tak	SPEŁNIA TAK /NIE
5.	Zarządzany w chmurze	Tak	SPEŁNIA TAK /NIE
6.	Zarządzanie przez stronę www	Tak	SPEŁNIA TAK /NIE
7.	Inspekcja ARP	Tak	SPEŁNIA TAK /NIE
8.	Konfigurowanie ustawień lokalizacji (CLI)	Tak	SPEŁNIA TAK /NIE
9.	Obsługa MIB	Tak	SPEŁNIA TAK /NIE
10.	<b>OCHRONA</b>		
11.	Funkcje DHCP	DHCP relay, DHCP server, DHCPv6 client	SPEŁNIA TAK /NIE
12.	Lista kontrolna dostępu (ACL)	Tak	SPEŁNIA TAK /NIE
13.	Zasady Listy Kontroli Dostępu (ACL)	1024	SPEŁNIA TAK /NIE
14.	IGMP snooping	Tak	SPEŁNIA TAK /NIE
15.	Ochrona hasłem	Tak	SPEŁNIA TAK /NIE
16.	obsługuje SSH/SSL	Tak	SPEŁNIA TAK /NIE
17.	Zabezpieczenie DoS	Tak	SPEŁNIA TAK /NIE
18.	Filtrowanie adresów MAC	Tak	SPEŁNIA TAK /NIE
19.	Szyfrowanie / bezpieczeństwo	HTTPS, SSH, SSL/TLS	SPEŁNIA TAK /NIE
20.	<b>PORTY I INTERFEJSY</b>		
21.	Podstawowe przełączanie RJ-45 Liczba portów Ethernet	48	SPEŁNIA TAK /NIE
22.	Podstawowe przełączania Ethernet RJ- 45 porty typ	Gigabit Ethernet (10/100/1000)	SPEŁNIA TAK /NIE
23.	Ilość slotów Modułu SFP+	4	SPEŁNIA TAK /NIE
24.	Liczba portów konsoli	RJ-45, USB typ C	SPEŁNIA TAK /NIE
25.	Wydajność	Przepustowość przełącznika nie może być mniejsza niż 176Gb/s. Szybkość przełączania ramek wewnątrz przełącznika nie może być mniejsza niż 130,9Mp/s.	SPEŁNIA TAK /NIE
26.	<b>SIEĆ</b>		
27.	Standardy komunikacyjne	EEE 802.1Q, IEEE 802.1ab, IEEE 802.1ad, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ad, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z	SPEŁNIA TAK /NIE
28.	Obsługa 10G	Tak	SPEŁNIA TAK



			/NIE
29.	Dublowanie portów	Tak	SPEŁNIA TAK /NIE
30.	Protokół drzewa rozpinającego	Tak	SPEŁNIA TAK /NIE
31.	Blokowanie head-of-line (HOL)	Tak	SPEŁNIA TAK /NIE
32.	Prędkość transferu danych przez Ethernet LAN	10,100,1000 Mbit/s	SPEŁNIA TAK /NIE
33.	Kontrola wzrostu natężenia ruchu	Tak	SPEŁNIA TAK /NIE
34.	Automatyczne MDI/MDI- X	Tak	SPEŁNIA TAK /NIE
35.	Podpora kontroli przepływu	Tak	SPEŁNIA TAK /NIE
36.	Agregator połączenia	Tak	SPEŁNIA TAK /NIE
37.	Obsługa sieci VLAN	Tak	SPEŁNIA TAK /NIE
38.	Liczba VLANs	4094	SPEŁNIA TAK /NIE
39.	<b>PRZESYŁANIE DANYCH</b>		
40.	Wielkość tabeli adresów	16000 wejścia	SPEŁNIA TAK /NIE
41.	Zgodny z Jumbo Frames	Tak	SPEŁNIA TAK /NIE
42.	Rozszerzenie Jumbo Frames	9000	SPEŁNIA TAK /NIE
43.	<b>FUNKCJE MULTICAST</b>		
44.	Obsługa Multicast	Tak	SPEŁNIA TAK /NIE
45.	<b>PROTOKOŁY</b>		
46.	Protokoły zarządzające	CLI, SNMP, Telnet, SSH, SSH-2, DHCP, SCP, HTTPS, HTTP, ICMP, TFTP, Syslog, SNMP 2c, SNMP 3, RMON, RADIUS	SPEŁNIA TAK /NIE
47.	<b>KONSTRUKCJA</b>		
48.	Możliwości montowania w stelażu	Tak	SPEŁNIA TAK /NIE
49.	Przycisk reset	Tak	SPEŁNIA TAK /NIE
50.	Diody LED	Tak	SPEŁNIA TAK /NIE
51.	<b>WYDAJNOŚĆ</b>		
52.	Procesor wbudowany wielordzeniowy	Tak	SPEŁNIA TAK /NIE
53.	Taktowanie procesora	1.4 GHz	SPEŁNIA TAK /NIE
54.	Pojemność pamięci flash	1 GB	SPEŁNIA TAK /NIE
55.	Pojemność pamięci RAM	1 GB	SPEŁNIA TAK /NIE
56.	Aktualizacje oprogramowania urządzenia	Tak	SPEŁNIA TAK /NIE

57.	<b>MOC</b>		
58.	Zasilacz dołączony	Tak	SPEŁNIA TAK /NIE
59.	<b>GWARANCJA</b>		
60.	Gwarancja	Dożywotnia producenta (min. do 60 miesięcy od wycofania z produkcji/sprzedaży przez producenta)	SPEŁNIA TAK /NIE

## 8 UPS CENTRALNY – 1 KPL.

L.P.	Parametr	Wymagania minimalne	
1.	Moc pozorna	min. 6000VA	Producent
			Model
2.	Moc rzeczywista	min. 6000W	Spełnia TAK/NIE
3.	Technologia	on-line (VFI), podwójna konwersja	Spełnia TAK/NIE
4.	Sprawność max (dla VFI)	> 92 %	Spełnia TAK/NIE
5.	Typ obudowy	rack/tower	Spełnia TAK/NIE
6.	Poziom hałasu	< 55dB	Spełnia TAK/NIE
7.	<b>parametry wejściowe</b>		Spełnia TAK/NIE
8.	Napięcie wejściowe	208 V AC / 220 V AC / 230 V AC / 240 V AC	Spełnia TAK/NIE
9.	Zakres napięcia wejściowego	80-300 V AC	Spełnia TAK/NIE
10.	Zakres częstotliwości wejściowej	45~55 / 54~66 Hz	Spełnia TAK/NIE
11.	<b>parametry wyjściowe</b>		Spełnia TAK/NIE
12.	Zakres napięcia wyjściowego	208 V AC / 220 V AC / 230 V AC / 240 V AC	Spełnia TAK/NIE
13.	Częstotliwość napięcia wyjściowego	50 / 60 Hz (+/- 0,5%)	Spełnia TAK/NIE
14.	Kształt napięcia wyjściowego	sinusoidalny	Spełnia TAK/NIE
15.	Czas przełączania sieć – UPS	0ms	Spełnia TAK/NIE
16.	Współczynnik odkształceń THDv	<2% liniowe obciążenie; < 5% @ nieliniowe obciążenie	Spełnia TAK/NIE
17.	Przeciążalność w trybie sieciowym	minimum 105-110% = 10 min, 110-130% = 1 min, >130% = przejście w bypass po 3 sek.	Spełnia TAK/NIE
18.	Przeciążalność w trybie bateryjnym	minimum 105-110% = 10 min, 110-130% = 1 min, >130% = przejście w bypass po 3 sek.	Spełnia TAK/NIE
19.	Baterie wewnętrzne w UPS lub w zewnętrznym module bateryjnym	minimum 12V 9Ah; szczelne, bezobsługowe	Spełnia TAK/NIE
20.	Czas podtrzymania (dla 50 % Pmax) - przy zastosowaniu baterii wew. lub z 1 zewnętrznym modulem bateryjnym	minimum 9 min	Spełnia TAK/NIE
21.	Możliwość podłączenie zewnętrznych modułów bateryjnych	wymagane	Spełnia TAK/NIE
22.	Możliwość włączenia testu baterii	wymagane	Spełnia

## Załącznik Nr 8

			TAK/NIE
pozostałe			
23.	Wejście zasilania	listwa zaciskowa / terminal śrubowy	Spełnia TAK/NIE
24.	Ilość i typ gniazd wyjściowych	listwa zaciskowa / terminal śrubowy oraz 4x IEC320 C19 + 2x IEC320 C13	Spełnia TAK/NIE
25.	Sygnalizacja	Wyświetlacz LCD, akustyczna	Spełnia TAK/NIE
26.	Informacje do odczytania z poziomu LCD	minimum napięcie wejściowe i wyjściowe, częstotliwość wejściowa i wyjściowa, obciążenie w procentach oraz obciążenie w watach lub kilowatach, praca w trybie sieciowym, bateryjnym, ECO, BYPASS, procentowa pojemność baterii, napięcie baterii, błąd baterii, niski poziom baterii, przeciążenie, pozostały czas pracy bateryjnej w minutach	Spełnia TAK/NIE
27.	Test baterii	wymagana możliwość ustawienia automatycznego testu baterii w zakresie 1 do 45 dni	Spełnia TAK/NIE
28.	Możliwość pracy w trybie konwertera częstotliwości	wymagane	Spełnia TAK/NIE
29.	Automatyczne ładowanie po powrocie zasilania	wymagane	Spełnia TAK/NIE
30.	Automatyczne uruchomienie po powrocie zasilania	wymagane	Spełnia TAK/NIE
31.	Interfejs komunikacyjny	RS232, USB, SNMP	Spełnia TAK/NIE
32.	Funkcja ROO - zdalne włączenie / wyłączenie zasilania	wymagane	Spełnia TAK/NIE
33.	Wymagania odnośnie interfejsu sieciowego	obsługa protokołu SNMP v1 i v3, HTTP/HTTPS, SSH	Spełnia TAK/NIE
		wsparcie dla IPv4 oraz IPv6	
		możliwość ustawienia hasła o długości 8 znaków	
		możliwość wyłączenia wybranych kanałów komunikacyjnych z urządzeniem	
		wsparcie dla LDAP lub RADIUS	
		dostęp do bazy danych MIB zgodnej z RFC 1628	
34.	Złącze EPO	wymagane	Spełnia TAK/NIE
35.	Wsporniki do montażu w szafie RACK	wymagane	Spełnia TAK/NIE
36.	Zewnętrzny bypass serwisowy w wersji rack lub naściennej, tego samego producenta co oferowany UPS	wymagany	Spełnia TAK/NIE
37.	Waga UPS	do 15kg	Spełnia TAK/NIE
38.	Wymiary UPS - wersja RACK	nie większe niż: wysokość 3U; głębokość 700 mm	Spełnia TAK/NIE
39.	Waga Moduł Bateryjny - jeżeli występuje	do 70 kg	Spełnia TAK/NIE
40.	Wymiary Moduł Bateryjny - wersja RACK - jeżeli występuje	nie większe niż: wysokość 3U; głębokość 700 mm	Spełnia TAK/NIE
41.	Gwarancja	minimum 24 miesiące na elektronikę i 24 miesiące na baterie	Spełnia TAK/NIE
42.	Serwis	autoryzowany serwis producenta zlokalizowany w Polsce.	Spełnia TAK/NIE
		naprawa w maksymalnie 5 dni roboczych	
		serwis realizowany w systemie door to door	



## Załącznik Nr 8

43.	Oprogramowanie	wsparcie dla systemów: Windows, Linux	Spełnia TAK/NIE
		wymagane wsparcie producenta w języku polskim (telefoniczne oraz mailowe)	
44.	Oświadczenia / dokumenty	oświadczenie producenta lub wyłącznego dystrybutora o spełnieniu minimalnych wymaganych parametrów specyfikacji	Spełnia TAK/NIE
		dla gwarancja standardowej lub rozszerzonej wymagane jest by realizowana była wyłącznie przez autoryzowany serwis producenta - należy przedstawić odpowiednie oświadczenie producenta lub wyłącznego dystrybutora	
		certyfiat lub oświadczenie producenta lub wyłącznego dystrybutora o posiadaniu przez oferenta statusu Autoryzowanego Partnera - mającego wiedzę w zakresie doboru i sprzedaży zasilania gwarantowanego (UPS) jeżeli oferent nie jest producentem sprzętu. deklaracja zgodności CE	
45.	Dodatkowe usługi	Podłączenie do przygotowanej instalacji elektrycznej (wyprowadzonych przez zamawiającego kabli). Podłączenie wyłącznie przez Autoryzowany Serwis Producenta uwzględniające podłączenie UPS, podłączenie modułu bateryjnego (jeżeli występuje), podłączenie bypassu do wejścia zasilania oraz do UPSa (jeżeli występuje), montaż w szafie rack, pierwsze uruchomienie, szkolenie z obsługi	Spełnia TAK/NIE

## 9 ZASADA RÓWNOWAŻNOŚCI ROZWIĄZAŃ I NEUTRALNOŚCI TECHNOLOGICZNEJ.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań lub też stosowane jest w celu wskazania aktualnie użytkowanego środowiska Zamawiającego, z którym rozwiązanie równoważne powinno być kompatybilne.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.
5. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.

## Załącznik Nr 8

9. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia poprawności przeprowadzonych testów może wezwać Wykonawcę do przedstawienia wskazanego przez Zamawiającego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowania overclockingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
10. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający dopuszcza równoważne im testy wydajnościowe umożliwiające potwierdzenie zakładanych poziomów wydajności. W przypadku użycia przez Wykonawcę równoważnych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia równoważności przeprowadzonych testów Wykonawca może zostać wezwany do dostarczenia Zamawiającemu wskazanego przez Zamawiającego oprogramowania testującego i równoważnego do niego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowania overclockingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
11. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązanie równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.
12. Za równoważną do normy ISO 9001 Zamawiający uzna normę, która dotyczy zarządzania jakością ustanawiając wymagania dla systemów zarządzania jakością w organizacjach w minimum następującym zakresie:
- 1) Skupienie na użytkowniku – Podstawowym celem systemu zarządzania jakością jest zwiększenie satysfakcji użytkownika poprzez spełnianie jego wymagania oraz oczekiwania. Organizacja powinna monitorować potrzeby użytkowników i dostarczać produkty lub usługi, które je zaspokajają.
  - 2) Przywództwo – Wspieranie kierownictwa w zapewnianiu odpowiednich zasobów i wsparcia w procesach zarządzania jakością. Przywódcy powinni tworzyć środowisko, które wspiera zaangażowanie pracowników w poprawę jakości.
  - 3) Zaangażowanie ludzi – Organizacja powinna zapewnić, aby wszyscy pracownicy byli zaangażowani w realizację celów jakościowych. Kluczowym elementem jest angażowanie personelu w procesy poprawy jakości i podejmowanie działań na rzecz doskonalenia.
  - 4) Podejście procesowe – Norma podkreśla, że organizacja powinna zarządzać swoimi procesami w sposób spójny i skuteczny, traktując je jako powiązane ze sobą elementy systemu zarządzania jakością, które wspólnie prowadzą do osiągnięcia celów organizacji.
  - 5) Podejście systemowe do zarządzania – Organizacja powinna traktować system zarządzania jakością jako całość, złożoną z wzajemnie powiązanych elementów (np. procesów, zasobów, technologii), które muszą działać w harmonii, aby osiągnąć cele jakościowe.
  - 6) Ciągłe doskonalenie – dążenie do ciągłego doskonalenia procesów w organizacji. Ciągłe doskonalenie jest kluczowym elementem skutecznego zarządzania jakością i poprawy wyników.
  - 7) Podejście do podejmowania decyzji oparte na faktach – w procesie podejmowania decyzji organizacja powinna opierać się na danych i analizach, a nie na przypuszczeniach czy intuicji. Podejście to pozwala na bardziej precyzyjne i obiektywne decyzje.
  - 8) Relacje z dostawcami na zasadzie wzajemnych korzyści – tworzenie partnerskich relacji z dostawcami, które będą korzystne dla obu stron. Współpraca z dostawcami powinna być oparta na zaufaniu i dążeniu do wspólnych celów jakościowych.
  - 9) Zarządzanie ryzykiem – norma wymaga, aby organizacje identyfikowały, oceniały i zarządzały ryzykiem związanym z procesami oraz ich wpływem na zdolność organizacji do dostarczania produktów i usług o wymaganej jakości.



## Załącznik Nr 8

- 10) Dokumentowanie systemu zarządzania jakością – Norma określa wymagania dotyczące dokumentowania systemu zarządzania jakością, w tym tworzenia polityki jakości, procedur, instrukcji roboczych oraz zapisów, które umożliwiają monitorowanie i weryfikację skuteczności systemu.
13. Za równoważną do normy ISO 50001 Zamawiający uzna normę, która dotyczy zarządzania energią w organizacjach w minimum następującym zakresie:
  - 1) Skupienie na poprawie efektywności energetycznej – Celem normy jest poprawa efektywności wykorzystania energii poprzez identyfikację obszarów, w których możliwe są oszczędności i usprawnienia w zarządzaniu energią.
  - 2) Zarządzanie cyklem życia energii – uwzględnia cały cykl życia energii, od planowania, poprzez wykorzystanie, aż po monitorowanie, ocenę i doskonalenie działań mających na celu zmniejszenie zużycia energii.
  - 3) Zintegrowane podejście z innymi systemami zarządzania – Norma jest zaprojektowana w sposób zgodny z innymi międzynarodowymi normami, co umożliwia integrację systemów zarządzania w organizacji.
  - 4) Podejście oparte na cyklu PDCA (Plan-Do-Check-Act) – opiera się na cyklu PDCA, który wspiera organizację w procesie ciągłego doskonalenia zarządzania energią poprzez planowanie, wdrażanie, monitorowanie i działania korygujące.
  - 5) Zaangażowanie kierownictwa – Norma wymaga, aby najwyższe kierownictwo organizacji angażowało się w proces zarządzania energią, podejmując decyzje, dostarczając zasoby oraz ustalając cele i polityki energetyczne.
  - 6) Ustalenie polityki energetycznej – norma zachęca organizację do opracowania polityki energetycznej, która definiuje kierunki działań, cele efektywności energetycznej oraz zobowiązania do ciągłego doskonalenia.
  - 7) Identyfikacja i ocena aspektów energetycznych – Norma wymaga przeprowadzenia analizy aspektów energetycznych, które mają istotny wpływ na zużycie energii i środowisko, oraz wdrożenia działań na rzecz ich poprawy.
  - 8) Monitorowanie, pomiar i analiza – nakłada obowiązek monitorowania i mierzenia zużycia energii oraz wydajności energetycznej organizacji. Organizacja powinna także stosować odpowiednie narzędzia do analizy wyników, identyfikacji możliwości poprawy oraz podejmowania działań korygujących.
  - 9) Zarządzanie ryzykiem i szansami – Norma podkreśla znaczenie identyfikacji ryzyk i szans związanych z zarządzaniem energią, a także działań na rzecz minimalizowania ryzyka i maksymalizowania możliwości poprawy efektywności energetycznej.
  - 10) Ciężar działań edukacyjnych i szkoleń – Norma wskazuje na konieczność zapewnienia odpowiedniego poziomu wiedzy i umiejętności w zakresie zarządzania energią dla wszystkich pracowników organizacji. Szkolenia i podnoszenie świadomości energetycznej są kluczowe dla skutecznego wdrażania polityki energetycznej.
14. Za równoważną do normy ISO 14001 Zamawiający uzna normę, która dotyczy systemów zarządzania środowiskowego w minimum następującym zakresie:
  - 1) Zarządzanie środowiskowe oparte na cyklu PDCA (Plan-Do-Check-Act) – norma opiera się na cyklu PDCA, który wspiera organizację w systematycznym zarządzaniu i doskonaleniu ich działań na rzecz ochrony środowiska. Proces obejmuje planowanie, wdrażanie, monitorowanie oraz podejmowanie działań korygujących.
  - 2) Zobowiązanie organizacji do ochrony środowiska – Norma wymaga, aby organizacja była zobowiązana do minimalizowania negatywnego wpływu na środowisko. To zobowiązanie powinno być wyrażone poprzez politykę środowiskową, która wskazuje na cele ochrony środowiska.
  - 3) Identyfikacja aspektów środowiskowych – Organizacja musi identyfikować i oceniać aspekty środowiskowe związane z jej działalnością, produktami i usługami. Ocena powinna uwzględniać wpływ na środowisko, zarówno w zakresie zużycia zasobów, jak i wytwarzania odpadów oraz emisji.
  - 4) Zgodność z przepisami prawnymi i innymi wymaganiami – norma wymaga, aby organizacja przestrzegała obowiązujących przepisów prawnych dotyczących ochrony środowiska oraz innych zobowiązań, które organizacja uzna za stosowne (np. normy branżowe).
  - 5) Cele środowiskowe i planowanie działań – Organizacja musi wyznaczać mierzalne cele środowiskowe i opracować plany działań, które pozwolą osiągnąć te cele. Cele te powinny być zgodne z polityką środowiskową i uwzględniać aspekt środowiskowy w całym cyklu życia produktów i usług.
  - 6) Zaangażowanie kierownictwa – zaangażowanie najwyższego kierownictwa w wdrażanie systemu zarządzania środowiskowego. Kierownictwo powinno zapewnić zasoby, nadzór i wspierać działania na rzecz ochrony środowiska.
  - 7) Zarządzanie ryzykiem środowiskowym – Norma podkreśla konieczność identyfikacji i oceny ryzyk środowiskowych związanych z działalnością organizacji. Organizacja powinna podejmować działania na rzecz minimalizowania ryzyk, a także wdrażać procedury zapobiegania i reagowania na sytuacje kryzysowe.
  - 8) Monitorowanie, pomiar i analiza wyników – Organizacja jest zobowiązana do monitorowania i mierzenia skuteczności swoich działań środowiskowych. Obejmuje to ocenę wpływu działań na środowisko, skuteczność realizacji celów oraz identyfikację obszarów do poprawy.
  - 9) Działania korygujące i zapobiegawcze – norma wymaga, aby organizacja wdrażała procedury podejmowania działań korygujących w przypadku niezgodności oraz działań zapobiegawczych, aby uniknąć powtarzania się problemów środowiskowych w przyszłości.
  - 10) Ciągłe doskonalenie systemu zarządzania środowiskowego – Podstawowym celem normy jest dążenie do ciągłego doskonalenia systemu zarządzania środowiskowego. Organizacja powinna regularnie przeglądać i aktualizować swoje cele, polityki i procesy, aby dostosować je do zmieniających się warunków środowiskowych oraz wymagań prawnych.
15. Za równoważną do normy ISO 27001 Zamawiający uzna normę, która określa standard zarządzania bezpieczeństwem informacji w minimum następującym zakresie: Zarządzanie ryzykiem – norma stosuje podejście oparte na zarządzaniu ryzykiem. Organizacja musi przeprowadzać ocenę ryzyka dla bezpieczeństwa informacji i podejmować odpowiednie środki w celu zarządzania tym ryzykiem.
  - 1) Ochrona informacji – Norma zapewnia, że organizacja identyfikuje, ocenia i zabezpiecza informacje, w tym dane osobowe, finansowe, techniczne, i inne zasoby przed zagrożeniami.
  - 2) Ciągłość działania – norma kładzie nacisk na ciągłość działania w przypadku awarii systemów, katastrof naturalnych, ataków cybernetycznych itp. Organizacje muszą przygotować plany awaryjne i procedury odzyskiwania danych.



- 3) Zaangażowanie kierownictwa – Norma wymaga aktywnego zaangażowania najwyższego kierownictwa w procesie zarządzania bezpieczeństwem informacji.
  - 4) Ciągłe doskonalenie – norma promuje ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji, aby dostosować go do zmieniających się zagrożeń i wymagań.
  - 5) Polityki bezpieczeństwa informacji – norma określa, że organizacja musi opracować i wdrożyć formalne polityki bezpieczeństwa informacji, które są zgodne z jej celami biznesowymi i wymaganiami regulacyjnymi.
  - 6) Szkolenia i świadomość pracowników – norma kładzie nacisk na edukację i szkolenia pracowników w zakresie bezpieczeństwa informacji. Wszyscy pracownicy muszą być świadomi swoich obowiązków w zakresie ochrony danych.
  - 7) Zarządzanie dostępem – norma wymaga, aby dostęp do informacji i zasobów organizacji był kontrolowany i ograniczony na podstawie ról i odpowiedzialności pracowników.
  - 8) Monitorowanie i przeglądy – norma określa, że organizacje muszą regularnie monitorować skuteczność wdrożonego systemu zarządzania bezpieczeństwem informacji oraz przeprowadzać audyty, które pozwolą ocenić zgodność z wymaganiami normy.
  - 9) Zgodność z przepisami prawa – norma wymaga, aby organizacje zapewniały zgodność z obowiązującymi przepisami prawnymi dotyczącymi ochrony danych osobowych, ochrony prywatności i bezpieczeństwa informacji.
16. Za równoważną do regulacji RoHS Zamawiający uzna regulację, która dotyczy stosowania substancji niebezpiecznych w sprzęcie elektrycznym i elektronicznym w minimum następującym zakresie:
- 1) Zakaz stosowania niebezpiecznych substancji – ogranicza użycie sześciu substancji niebezpiecznych w sprzęcie elektrycznym i elektronicznym: ołów (Pb), rtęć (Hg), kadm (Cd), sześciowartościowy chrom (Cr<sup>6</sup>), polibromowane bifenyle (PBB) i polibromowane etery difenyłowe (PBDE).
  - 2) Zastosowanie do sprzętu elektronicznego i elektrycznego – obejmuje szeroki zakres produktów, takich jak telewizory, komputery, sprzęt AGD, zabawki, oświetlenie LED, urządzenia medyczne, sprzęt telekomunikacyjny i inne urządzenia elektroniczne.
  - 3) Zobowiązanie producentów do zgodności – Producenci i importerzy sprzętu elektrycznego i elektronicznego muszą zapewnić, że ich produkty nie zawierają zabronionych substancji powyżej dopuszczalnych poziomów.
  - 4) Oświadczenia o zgodności – Producenci są zobowiązani do dostarczania odpowiednich oświadczeń o zgodności z regulacją. Powinny one być udostępniane organom nadzoru oraz użytkownikom w razie potrzeby.
  - 5) Kontrola i nadzór rynkowy – regulacja nakłada obowiązek przeprowadzania kontroli rynkowych przez odpowiednie organy państwowe, aby upewnić się, że produkty wprowadzane na rynek UE spełniają wymogi dyrektywy.
  - 6) Ograniczenie wpływu na zdrowie i środowisko – celem regulacji jest zmniejszenie negatywnego wpływu niebezpiecznych substancji na zdrowie ludzi oraz na środowisko naturalne, szczególnie podczas recyklingu i utylizacji odpadów elektronicznych.
  - 7) Zdolność do recyklingu i odzysku – regulacja promuje projektowanie produktów w sposób, który umożliwia ich łatwiejszy recykling i utylizację. Przepisy zakładają, że zabronione substancje nie mogą występować w produktach w ilościach, które utrudniają ich odzyskiwanie.
  - 8) Zakres geograficzny – regulacja ma zastosowanie w krajach Unii Europejskiej oraz w krajach, które przyjęły odpowiednie przepisy zgodne z dyrektywą.
  - 9) Obowiązki w przypadku modyfikacji produktów – W przypadku wprowadzenia istotnych zmian w produkcie (np. zmiana jego konstrukcji), producent musi upewnić się, że nowa wersja również spełnia wymagania regulacji. Dotyczy to również produktów wprowadzanych na rynek wtórny (np. w ramach naprawy lub refabrykacji).
17. Za równoważną do regulacji CE Zamawiający uzna regulację, która spełnia wszystkie odpowiednie wymagania dotyczące zdrowia, bezpieczeństwa oraz ochrony środowiska, zgodnie z przepisami UE w minimum następującym zakresie:
- 1) Potwierdzenie zgodności z wymaganiami UE – formalne oświadczenie producenta lub importera, że dany produkt spełnia wszystkie obowiązujące przepisy unijne dotyczące zdrowia, bezpieczeństwa, ochrony środowiska i innych przepisów regulujących dany produkt.
  - 2) Oznakowanie CE – posiada system oznaczeń, który wskazuje, że produkt przeszedł ocenę zgodności i jest dopuszczony do sprzedaży w Unii Europejskiej.
  - 3) Szczegółowe informacje o producencie – dokument potwierdzający musi zawierać pełne dane producenta (lub importera), takie jak nazwa firmy, adres siedziby, a także dane kontaktowe. W przypadku importera – także informacje o tym, kto odpowiada za dany produkt w UE.
  - 4) Opis produktu – dokument potwierdzający musi zawierać szczegółowy opis produktu, który obejmuje nazwę produktu, numer referencyjny lub numer katalogowy, a także inne identyfikatory, które umożliwiają jednoznaczną identyfikację produktu.
  - 5) Odniesienia do odpowiednich norm – dokument potwierdzający wskazuje normy, dyrektywy lub przepisy unijne, z którymi produkt jest zgodny.
  - 6) Procedura oceny zgodności – dokument potwierdzający musi wskazywać, w jaki sposób ocena zgodności produktu została przeprowadzona (np. przez samodzielną ocenę producenta lub poprzez współpracę z jednostką notyfikowaną w przypadku bardziej skomplikowanych produktów).
  - 7) Data i miejsce sporządzenia deklaracji – dokument potwierdzający powinien zawierać datę sporządzenia deklaracji oraz miejsce jej podpisania, co ma znaczenie prawne i daje pewność co do okresu ważności oświadczenia.
  - 8) Podpis osoby upoważnionej – dokument potwierdzający musi być podpisana przez osobę upoważnioną w imieniu producenta lub importera, która jest odpowiedzialna za prawdziwość oświadczenia. Zwykle jest to przedstawiciel firmy, który ma uprawnienia do składania oświadczeń w imieniu organizacji.
  - 9) Wymóg dostępności dla organów nadzoru – dokument potwierdzający musi być dostępny dla odpowiednich organów nadzoru rynkowego, które mogą przeprowadzać kontrole w celu weryfikacji zgodności produktów z obowiązującymi wymaganiami.

## Załącznik Nr 8

- 10) Zakres odpowiedzialności producenta – dokument potwierdzający musi być dokumentem, który wiąże producenta z odpowiedzialnością za zgodność produktu z wymaganiami prawnymi i normatywnymi. Jeżeli produkt nie spełnia wymagań, producent lub importer mogą być pociągnięci do odpowiedzialności za naruszenie przepisów UE.
18. Za równoważną do certyfikacji FIPS 140-2 Zamawiający uzna certyfikację, która dotyczy standardu wymagań bezpieczeństwa dla modułów kryptograficznych w minimum następującym zakresie:
- 1) Obejmuje wszystkie komponenty sprzętowe, oprogramowanie i kombinacje tych elementów, które realizują operacje kryptograficzne (np. szyfrowanie, podpisy cyfrowe, generowanie kluczy).
  - 2) Wymaga, aby moduły kryptograficzne posiadały odpowiednią ochronę przed manipulacjami fizycznymi.
  - 3) Wymaga, aby wszystkie klucze kryptograficzne były odpowiednio chronione. Obejmuje to m.in. przechowywanie, generowanie, zarządzanie i wymianę kluczy w sposób, który zapobiega ich nieautoryzowanemu ujawnieniu.
  - 4) Nakłada wymagania dotyczące bezpiecznego uruchamiania modułu kryptograficznego, w tym procedury inicjalizacji, które muszą zapewniać, że urządzenie jest w pełni zabezpieczone przed uruchomieniem jakichkolwiek operacji kryptograficznych.
  - 5) Wymaga, aby systemy kryptograficzne były testowane pod kątem zabezpieczeń kryptograficznych.
  - 6) Definiuje wymagania dotyczące implementacji standardowych algorytmów kryptograficznych.
  - 7) Wymaga, aby systemy kryptograficzne były odpowiednio utrzymywane przez cały okres ich użytkowania.





## Załącznik nr 8 - Klauzula informacyjna FERC

### Klauzula informacyjna FERC

W celu wykonania obowiązku nałożonego w drodze art. 13 i 14 RODO, w związku z art. 88 ustawy wdrożeniowej, informujemy o zasadach przetwarzania Państwa danych osobowych:

#### Administrator danych

Odrębnymi administratorami Państwa danych są:

1. Minister Funduszy i Polityki Regionalnej (dalej jako MFiPR), w zakresie w jakim pełni funkcję Instytucji Zarządzającej (IZ) Funduszami Europejskimi na Rozwój Cyfrowy 2021-2027 (dalej jako FERC) z siedzibą przy ul. Wspólnej 2/4, 00-926 Warszawa,
2. Centrum Projektów Polska Cyfrowa (dalej jako CPPC) w zakresie w jakim pełni funkcje Instytucji Pośredniczącej (IP) FERC, z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa,
3. Centrum Projektów Polska Cyfrowa (dalej jako CPPC) w zakresie w jakim pełni funkcje Beneficjenta FERC, z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa.

#### Cel przetwarzania danych

Państwa dane osobowe będziemy przetwarzać w związku z realizacją FERC, w szczególności w związku z naborem 2.2 FERC. Podanie danych jest dobrowolne, ale konieczne do realizacji ww. celu. Odmowa ich podania jest równoznaczna z brakiem możliwości podjęcia stosownych działań.

#### Podstawa przetwarzania

Będziemy przetwarzać Państwa dane osobowe w związku z tym, że:

1. Zobowiązuje nas do tego **prawo** (art. 6 ust. 1 lit. c RODO):
  - 1) art. 87 ustawy wdrożeniowej,
  - 2) art. 61 ustawy z 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz. U. z 2022 r. poz. 1079),
  - 3) ustawa z 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (tekst jednolity Dz.U. z 2023 r. poz. 775 z późn. zm.),

- 4) art. 206 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (tekst jednolity Dz. U. z 2022 r. poz. 1634, z późn. zm.),
  - 5) Porozumienie trójstronne w sprawie systemu realizacji programu „Fundusze Europejskie na Rozwój Cyfrowy 2021-2027” z 2.02.2023 r.,
  - 6) rozporządzenia Ministra Cyfryzacji z dnia 16 lutego 2023 r. w sprawie udzielania pomocy na rozwój infrastruktury szerokopasmowej w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (Dz. U. z 2023 r. poz. 405),
2. Wykonujemy zadania w interesie publicznym lub sprawujemy powierzoną nam władzę publiczną (art. 6 ust. 1 lit. e RODO),
  3. Przygotowujemy i realizujemy umowy, których są Państwo stroną, a przetwarzanie danych osobowych jest niezbędne do ich zawarcia i wykonania (art. 6 ust. 1 lit. b RODO).

### Rodzaje przetwarzanych danych

Możemy przetwarzać następujące rodzaje Państwa danych:

1. dane identyfikacyjne, wskazane w art. 87 ust. 2 pkt 1 ustawy wdrożeniowej, w tym: imię, nazwisko, adres, adres poczty elektronicznej, numer telefonu, numer faksu, PESEL, REGON, wykształcenie, identyfikatory internetowe,
2. dane związane z zakresem uczestnictwa osób fizycznych w projekcie, wskazane w art. 87 ust. 2 pkt 2 ustawy wdrożeniowej, w tym w szczególności: wynagrodzenie, formę i okres zaangażowania w projekcie,
3. dane osób fizycznych widniejące na dokumentach potwierdzających kwalifikowalność wydatków, wskazane w art. 87 ust. 2 pkt. 3 ustawy wdrożeniowej, m.in. numer rachunku bankowego, doświadczenie zawodowe, numer uprawnień budowlanych, numer księgi wieczystej,
4. dane dotyczące wizerunku i głosu osób uczestniczących w realizacji Programu lub biorących udział w wydarzeniach z nim związanych.

Dane pozyskujemy bezpośrednio od osób, których one dotyczą, albo od instytucji i podmiotów zaangażowanych w realizację FERC w tym w szczególności od wnioskodawców, beneficjentów, partnerów.

## **Dostęp do danych osobowych**

Dostęp do Państwa danych osobowych mają pracownicy i współpracownicy MFiPR oraz CPPC.

Ponadto Państwa dane osobowe mogą być powierzane lub udostępniane:

1. podmiotom, w tym ekspertom, o których mowa w art. 80 ustawy wdrożeniowej, którym zleciliśmy wykonywanie zadań w ramach realizacji FERC,
2. instytucji audytowej, o której mowa w art. 71 rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1060 z dnia 24 czerwca 2021 r. ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji i Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury, a także przepisy finansowe na potrzeby tych funduszy oraz na potrzeby Funduszu Azylu, Migracji i Integracji, Funduszu Bezpieczeństwa Wewnętrznego i Instrumentu Wsparcia Finansowego na rzecz Zarządzania Granicami i Polityki Wizowej,
3. instytucjom Unii Europejskiej (UE) lub podmiotom, którym UE powierzyła zadania dotyczące wdrażania FERC;
4. podmiotom, które wykonują dla nas usługi związane z obsługą i rozwojem systemów teleinformatycznych, a także zapewnieniem łączności, np. dostawcom rozwiązań IT i operatorom telekomunikacyjnym.

## **Okres przechowywania danych**

Będziemy przechowywać Państwa dane osobowe zgodnie z przepisami o narodowym zasobie archiwalnym i archiwach, do momentu zakończenia realizacji przez IZ/IP/Beneficjenta wszelkich zadań związanych z realizacją i rozliczeniem FERC, z zastrzeżeniem przepisów, które mogą przewidywać dłuższy termin przeprowadzania kontroli, a ponadto przepisów dotyczących pomocy publicznej i pomocy *de minimis* oraz przepisów dotyczących podatku od towarów i usług.

## **Prawa osób, których dane dotyczą**

Przysługują Państwu następujące prawa:

1. dostępu do swoich danych osobowych oraz otrzymania ich kopii (art. 15 RODO),
2. do sprostowania swoich danych (art. 16 RODO),



3. do usunięcia swoich danych (art. 17 RODO) - jeśli dotyczy,
4. do żądania od administratora ograniczenia przetwarzania swoich danych (art. 18 RODO),
5. wniesienia sprzeciwu – wobec przetwarzania swoich danych (art. 21 RODO) - jeśli przetwarzanie odbywa się w celu wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, powierzonej administratorowi (tj. w celu, o którym mowa w art. 6 ust. 1 lit. e RODO,
6. wniesienia skargi do organu nadzorczego (art. 77 RODO), tj. Prezesa Urzędu Ochrony Danych Osobowych, w przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO lub inne przepisy prawa regulujące kwestię ochrony danych osobowych.

### **Zautomatyzowane podejmowanie decyzji**

Dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

### **Przekazywanie danych do państwa trzeciego**

Nie zamierzamy przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej innej niż Unia Europejska. W przypadku konieczności przekazania Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej zapewniamy, że odbędzie się to z zachowaniem warunków określonych w art. 45 lub 46 RODO.

### **Kontakt z administratorem danych i Inspektorem Ochrony Danych**

Jeśli mają Państwo pytania dotyczące przetwarzania przez CPPC danych osobowych, prosimy kontaktować z Inspektorami Ochrony Danych Osobowych (dalej jako IOD) w następujący sposób:

1. IOD MFiPR:
  - 1) pocztą tradycyjną kierując korespondencję na adres: ul. Wspólna 2/4, 00-926 Warszawa,
  - 2) elektronicznie na adres e-mail: [IOD@mfipr.gov.pl](mailto:IOD@mfipr.gov.pl),
2. IOD CPPC:
  - 1) pocztą tradycyjną kierując korespondencję na adres: ul. Spokojna 13A, 01-044 Warszawa,
  - 2) elektronicznie na adres e-mail: [bezpieczenstwo@cppc.gov.pl](mailto:bezpieczenstwo@cppc.gov.pl).

**Podstawa prawna:**

1. ustawa wdrożeniowa - ustawa z 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz. U. z 2022 r., poz. 1079),
2. RODO - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Dz. Urz. UE. L 119 z 4 maja 2016 r., s.1-88; Dz. Urz. UE L 127 z 23 maja 2018, str. 2 oraz Dz. Urz. UE L 74 z 4 marca 2021, str. 35).

