



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Załącznik Nr 1 do SWZ

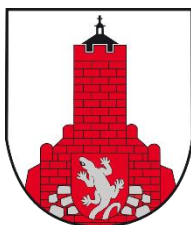
Numer sprawy: RGil.271.4.2025.MM

Lisewo, dnia 16 czerwca 2025 r.

Szczegółowy Opis Przedmiotu Zamówienia

na dostawę sprzętu i oprogramowania informatycznego oraz usługi związane
z realizacją projektu

„Cyberbezpieczny Samorząd w Gminie Lisewo”



Cyberbezpieczny
Samorząd

Spis treści

1. Zestawienie ilościowe.....	3
2. Zasada równoważności rozwiązań i neutralności technologicznej.	4
3. Opis przedmiotu zamówienia dla części nr 1.	16
3.1. Wymagania ogólne.....	16
3.2. Zakup klastra serwerowego (1 szt.).....	17
3.2.1. Zakup serwerów (2 szt.).....	17
3.2.2. Zakup macierzy dyskowej SAN (1 szt.).....	20
3.3. Zakup serwera (1 szt.).	21
3.4. Zakup przełącznika TYP A (3 szt.).....	24
3.5. Zakup przełącznika TYP B (1 szt.).....	25
3.6. Zakup NAS (1 szt.).....	26
3.7. Zakup UPS TYP A (1 szt.).	27
3.8. Zakup UPS TYP B (1 szt.).	28
3.9. Zakup tokenu (5 szt.).	29
3.10. Zakup access point (2 szt.).....	29
3.11. Zakup usług wdrożenia (1 szt.).	30
4. Opis przedmiotu zamówienia części nr 2.	31
4.1. Wymagania ogólne.....	31
4.2. Rozbudowa oprogramowania automatyzującego proces inwentaryzacji i monitorowania (1 szt.).	32

1. Zestawienie ilościowe.

Część nr 1 – Dostawa sprzętu i oprogramowania informatycznego.

Lp.	Nazwa	Ilość
1.	Zakup klastra serwerowego	1 szt.
2.	Zakup serwera	1 szt.
3.	Zakup przełącznika TYP A	3 szt.
4.	Zakup przełącznika TYP B	1 szt.
5.	Zakup NAS	1 szt.
6.	Zakup UPS TYP A	1 szt.
7.	Zakup UPS TYP B	1 szt.
8.	Zakup tokenu	5 szt.
9.	Zakup access point	2 szt.
10.	Zakup usług wdrożenia	1 szt.

Część nr 2 – Dostawa oprogramowania informatycznego.

Lp.	Nazwa	Ilość
1.	Rozbudowa oprogramowania automatyzującego proces inwentaryzacji i monitorowania	1 szt.

2. 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 wskazanym 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.
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:

- a. 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.
- b. Przywództwo – Wspieranie kierownictwa w zapewnianiu odpowiednich zasobów i wsparcia w procesach zarządzania jakością. Przywódcy powinni tworzyć środowisko, które wspiera zaangażowanie pracowników w poprawę jakości.
- c. 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.
- d. 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.
- e. 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.
- f. Ciągłe doskonalenie – dążenie do ciągłego doskonalenia procesów w organizacji. Ciągłe doskonalenie jest kluczowym elementem skutecznego zarządzania jakością i poprawy wyników.
- g. 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.
- h. 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.
- i. 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.
- j. 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:

- a. 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.

- b. 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.
 - c. Zintegrowane podejście z innymi systemami zarządzania – Norma jest zaprojektowana w sposób zgodny z innymi międzynarodowymi normami, co umożliwia integrację systemów zarządzania w organizacji.
 - d. 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.
 - e. Zaangażowanie kierownictwa – Norma wymaga, aby najwyższe kierownictwo organizacji angażowało się w proces zarządzania energią, podejmując decyzje, dostarczając zasoby oraz ustalając cele i polityki energetyczne.
 - f. Ustalenie polityki energetycznej – norma zachęca organizację do opracowania polityki energetycznej, która definiuje kierunki działań, cele efektywności energetycznej oraz zobowiązania do ciągłego doskonalenia.
 - g. 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.
 - h. 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.
 - i. 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.
 - j. 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:
- a. 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.
 - b. 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.
 - c. 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.
 - d. 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).
- e. 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.
 - f. Zaangażowanie kierownictwa – zaangażowanie najwyższego kierownictwa w wdrażanie systemu zarządzania środowiskowego. Kierownictwo powinno zapewnić zasoby, nadzór i wspierać działania na rzecz ochrony środowiska.
 - g. 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.
 - h. 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.
 - i. 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.
 - j. 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:
- a. 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.
 - b. Ochrona informacji – Norma zapewnia, że organizacja identyfikuje, ocenia i zabezpiecza informacje, w tym dane osobowe, finansowe, techniczne, i inne zasoby przed zagrożeniami.
 - c. 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.
 - d. Zaangażowanie kierownictwa – Norma wymaga aktywnego zaangażowania najwyższego kierownictwa w procesie zarządzania bezpieczeństwem informacji.
 - e. Ciągłe doskonalenie – norma promuje ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji, aby dostosować go do zmieniających się zagrożeń i wymagań.
 - f. 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.

- g. 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.
 - h. Zarządzanie dostępem – norma wymaga, aby dostęp do informacji i zasobów organizacji był kontrolowany i ograniczony na podstawie ról i odpowiedzialności pracowników.
 - i. 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.
 - j. 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:
- a. Zakaz stosowania niebezpiecznych substancji – ogranicza użycie sześciu substancji niebezpiecznych w sprzęcie elektrycznym i elektronicznym: ołów (Pb), rtęć (Hg), kadm (Cd), sześciowartościowy chrom (Cr⁶), polibromowane bifenyle (PBB) i polibromowane etery difenylowe (PBDE).
 - b. 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.
 - c. Zobowiązanie producentów do zgodności – Producenci i importerzy sprzętu elektrycznego i elektronicznego muszą zapewnić, że ich produkty nie zawierają zabronionych substancji powyżej dopuszczalnych poziomów.
 - d. 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.
 - e. 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.
 - f. 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.
 - g. 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.
 - h. Zakres geograficzny – regulacja ma zastosowanie w krajach Unii Europejskiej oraz w krajach, które przyjęły odpowiednie przepisy zgodne z dyrektywą.
 - i. 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:

- a. 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.
- b. Oznakowanie CE – posiada system oznaczeń, który wskazuje, że produkt przeszedł ocenę zgodności i jest dopuszczony do sprzedaży w Unii Europejskiej.
- c. 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.
- d. 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.
- e. Odniesienia do odpowiednich norm – dokument potwierdzający wskazuje normy, dyrektywy lub przepisy unijne, z którymi produkt jest zgodny.
- f. 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).
- g. 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.
- h. Podpis osoby upoważnionej – dokument potwierdzający musi być podpisany 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.
- i. 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.
- j. 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:

- a. Obejmuje wszystkie komponenty sprzętowe, oprogramowanie i kombinacje tych elementów, które realizują operacje kryptograficzne (np. szyfrowanie, podpisy cyfrowe, generowanie kluczy).
- b. Wymaga, aby moduły kryptograficzne posiadały odpowiednią ochronę przed manipulacjami fizycznymi.

- c. 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.
- d. 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.
- e. Wymaga, aby systemy kryptograficzne były testowane pod kątem zabezpieczeń kryptograficznych.
- f. Definiuje wymagania dotyczące implementacji standardowych algorytmów kryptograficznych.
- g. Wymaga, aby systemy kryptograficzne były odpowiednio utrzymywane przez cały okres ich użytkowania.

19. Minimalne kryteria równoważności dla urządzenia UTM Fortigate 60F:

- a. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.
- b. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trybów: Routera z funkcją NAT.
- c. System musi wspierać IPv4 oraz IPv6 w zakresie: firewall, ochrony w warstwie aplikacji, protokołów routingu dynamicznego.
- d. Redundancja, monitoring i wykrywanie awarii:
 - i. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – system musi zapewniać możliwość łączenia w klaster Active-Passive. Musi być dostępna funkcja synchronizacji sesji firewall,
 - ii. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych,
 - iii. Monitoring stanu realizowanych połączeń VPN.
- e. Interfejsy: co najmniej 5 x Ethernet 10/100/1000.
- f. Wydajność:
 - Przepustowość firewall – co najmniej 10 Gbps,
 - Liczba równoległych sesji – co najmniej 0,7 mln.
 - Przepustowość IPS – co najmniej 1,4 Gbps.
 - Liczba jednoczesnych klientów SSL VPN – co najmniej 200.
- g. Funkcje Systemu Bezpieczeństwa:
 - Kontrola Aplikacji,
 - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN,
 - Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS,
 - Ochrona przed atakami - Intrusion Prevention System,
 - Kontrola stron WWW,
 - Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP,
 - Zarządzanie pasmem (QoS, Traffic shaping),
 - Analiza ruchu szyfrowanego protokołem SSL.
- h. Polityki firewall:
 - Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, IPS i aplikacje, reakcje zabezpieczeń, rejestrowanie zdarzeń,

- System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz translację jeden do jeden oraz jeden do wielu,
 - W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
- i. Połączenia VPN:
- System musi umożliwiać konfigurację połączeń typu IPSec VPN,
 - System musi umożliwiać konfigurację połączeń typu SSL VPN.
- j. Routing i obsługa łączy WAN:
- W zakresie routingu rozwiązanie powinno zapewniać obsługę: routingu statycznego, Policy Based Routingu, protokołów dynamicznego routingu,
 - System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia.
- k. Kontrola antywirusowa:
- Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji,
 - Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji,
 - Moduł kontroli antywirusowej ma mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze w celu rozpoznawania zagrożeń.
- l. Ochrona przed atakami:
- Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych,
 - Baza sygnatur ataków musi być aktualizowana automatycznie,
 - System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
- m. Kontrola aplikacji:
- Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie analizy pakietów,
 - Baza Kontroli Aplikacji musi być aktualizowana automatycznie,
 - Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
- n. Kontrola WWW:
- W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware, phishing, spam, proxy avoidance. Jako rozwiązanie równoważne dopuszcza się realizację zapewnienia bezpieczeństwa w tych kategoriach na poziomie firewalla,
 - Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard,
 - Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL,
 - Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
- o. Uwierzytelnianie użytkowników w ramach sesji:
- System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą co najmniej haseł statycznych,

- Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory.
- p. Zarządzanie:
- Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego,
 - Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów,
 - Wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
- q. Urządzenie powinno umożliwiać monitorowania logów ruchu, administracja urządzenia musi być możliwe poprzez graficzny interfejs zarządzania, rozwiązanie powinno umożliwiać wysyłanie alarmów przez SNMP lub e-mail, urządzenie powinno mieć możliwość generowania raportów.
- r. W ramach Zamówienia Wykonawca dostarczy licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować kontrolę aplikacji, IPS, antywirus, antyspam, web filtering na okres 24 miesięcy.
- s. Urządzenie musi być objęte serwisem gwarancyjnym producenta na okres 24 miesięcy.
- t. W przypadku zaoferowania rozwiązania równoważnego Wykonawca jest zobligowany do instalacji, wdrożenia oraz migracji konfiguracji istniejącego urządzenia UTM oraz przeprowadzenia szkolenia dla administratora w zakresie konfiguracji i eksploatacji na podstawie wcześniej zaakceptowanego przez Zamawiającego zakresu merytorycznego szkolenia.

20. Minimalne kryteria równoważności dla urządzenia UTM Fortigate 40E:

- a. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.
- b. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trybów: Routera z funkcją NAT.
- c. System musi wspierać IPv4 oraz IPv6 w zakresie: firewall, ochrony w warstwie aplikacji, protokołów routingu dynamicznego.
- d. Redundancja, monitoring i wykrywanie awarii:
 - i. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – system musi zapewniać możliwość łączenia w klaster Active-Passive. Musi być dostępna funkcja synchronizacji sesji firewall,
 - ii. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych,
 - iii. Monitoring stanu realizowanych połączeń VPN.
- e. Interfejsy: co najmniej 5 x Ethernet 10/100/1000.
- f. Wydajność:
 - Przepustowość firewall – co najmniej 5 Gbps,
 - Liczba równoległych sesji – co najmniej 0,7 mln.
 - Przepustowość IPS – co najmniej 1 Gbps.
 - Liczba jednoczesnych klientów SSL VPN – co najmniej 200.
- g. Funkcje Systemu Bezpieczeństwa:
 - Kontrola Aplikacji,
 - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN,
 - Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS,

- Ochrona przed atakami - Intrusion Prevention System,
 - Kontrola stron WWW,
 - Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP,
 - Zarządzanie pasmem (QoS, Traffic shaping),
 - Analiza ruchu szyfrowanego protokołem SSL.
- h. Polityki firewall:
- Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, IPS i aplikacje, reakcje zabezpieczeń, rejestrowanie zdarzeń,
 - System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz translację jeden do jeden oraz jeden do wielu,
 - W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
- i. Połączenia VPN:
- System musi umożliwiać konfigurację połączeń typu IPSec VPN,
 - System musi umożliwiać konfigurację połączeń typu SSL VPN.
- j. Routing i obsługa łączy WAN:
- W zakresie routingu rozwiązanie powinno zapewniać obsługę: routingu statycznego, Policy Based Routingu, protokołów dynamicznego routingu,
 - System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia.
- k. Kontrola antywirusowa:
- Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji,
 - Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji,
 - Moduł kontroli antywirusowej ma mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze w celu rozpoznawania zagrożeń.
- l. Ochrona przed atakami:
- Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych,
 - Baza sygnatur ataków musi być aktualizowana automatycznie,
 - System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
- m. Kontrola aplikacji:
- Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie analizy pakietów,
 - Baza Kontroli Aplikacji musi być aktualizowana automatycznie,
 - Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
- n. Kontrola WWW:
- W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware, phishing, spam, proxy avoidance. Jako rozwiązanie równoważne dopuszcza się realizację zapewnienia bezpieczeństwa w tych kategoriach na poziomie firewalla,

- Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard,
 - Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL,
 - Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
- o. Uwierzytelnianie użytkowników w ramach sesji:
- System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą co najmniej haseł statycznych,
 - Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory.
- p. Zarządzanie:
- Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego,
 - Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów,
 - Wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
- q. Urządzenie powinno umożliwiać monitorowanie logów ruchu, administracja urządzenia musi być możliwa poprzez graficzny interfejs zarządzania, rozwiązanie powinno umożliwiać wysyłanie alarmów przez SNMP lub e-mail, urządzenie powinno mieć możliwość generowania raportów.
- r. W ramach Zamówienia Wykonawca dostarczy licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować kontrolę aplikacji, IPS, antywirus, antyspam, web filtering na okres 24 miesięcy.
- s. Urządzenie musi być objęte serwisem gwarancyjnym producenta na okres 24 miesięcy.
- t. W przypadku zaoferowania rozwiązania równoważnego Wykonawca jest zobligowany do instalacji, wdrożenia oraz migracji konfiguracji istniejącego urządzenia UTM oraz przeprowadzenia szkolenia dla administratora w zakresie konfiguracji i eksploatacji na podstawie wcześniej zaakceptowanego przez Zamawiającego zakresu merytorycznego szkolenia.

3. Opis przedmiotu zamówienia dla części nr 1.

3.1. 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 9 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. 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.
8. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi”, „powinien”, „możliwość” określając w ten sposób wymaganą funkcjonalność oprogramowania.

3.2. Zakup klastra serwerowego (1 szt.).

Klastrer serwerowy składa się z dwóch serwerów oraz macierzy dyskowej SAN i będzie wdrożony w serwerowni Urzędu Gminy w Lisewie. Wykonawca jest odpowiedzialny za dostarczenie, montaż, uruchomienie produkcyjne klastra i jego obowiązkiem jest dostarczenie wszystkich niezbędnych elementów i wykonanie wszystkich niezbędnych prac w celu uruchomienia klastra, w tym kabli połączeniowych, wkładek etc.

3.2.1. Zakup serwerów (2 szt.).

Minimalne parametry techniczne serwera:

1. Obudowa typu RACK o wysokości maksymalnie 2U z możliwością instalacji min. 16 dysków 2.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych wraz z podłączonymi przewodami.
2. Płyta główna z możliwością zainstalowania dwóch procesorów.
3. Zainstalowane dwa procesory klasy x86 dedykowane do pracy z oferowanym serwerem, umożliwiające osiągnięcie przez serwer wyniku co najmniej 175 punktów w teście SPECrate2017_int_base dla konfiguracji dwuprocesorowej według wyników publikowanych na stronie www.spec.org. Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie dla procesora dedykowanego do pracy z zaoferowanym serwerem żądanej przez Zamawiającego wydajności.
4. Pamięć RAM: zainstalowane min. 256 GB w najnowszej technologii oferowanej przez producenta, płyta główna musi obsługiwać do min. 2 TB pamięci RAM DDR5, co najmniej 15 slotów na pamięć wolnych w oferowanej konfiguracji.
5. Zabezpieczenia pamięci RAM: Memory Rank Sparing i/lub Memory Mirror i/lub Single Device Data Correction i/lub Memory Lockstep i/lub Chipkill i/lub Extended ECC i/lub Advanced Memory Device Correction i/lub AMD Memory Guard i/lub ECC i/lub Demand Scrubbing i/lub Patrol Scrubbing i/lub Permanent Fault Detection (PFD).
6. Zintegrowana karta graficzna ze złączem VGA.
7. Interfejsy sieciowe: Wbudowane co najmniej 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT, co najmniej 2 interfejsy w 10GbE w standardzie SFP+ z dedykowanymi wkładkami do każdego portu oraz co najmniej 2 interfejsy FC o prędkości transferu min. 16 Gb/s na port w celu podłączenia serwerów z macierzą dyskową SAN.
8. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 2 dyski twarde Hot-Plug SSD SATA o prędkości min. 6 Gb/s o pojemności co najmniej 480 GB każdy. W przypadku uszkodzenia dysku w okresie gwarancji Zamawiający wymaga by uszkodzony dysk pozostał jego własnością.
9. Kontroler RAID: Sprzętowy kontroler dyskowy umożliwiający konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60 z podtrzymaniem baterijnym.
10. Wbudowane porty: min. 3 porty USB, w tym co najmniej 1 port USB musi być dostępny z przodu obudowy. Ilość dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęźniaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera.
11. Wentylatory: typu Hot Plug.

12. Zasilacze: Redundantne typu Hot Plug o mocy nieprzekraczającej 1100 W każdy.
13. Karta/moduł zarządzania: Niezależny od zainstalowanego na serwerze systemu operacyjnego posiadający dedykowane złącze umożliwiające zdalne zarządzanie:
 - 1) zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
 - 2) zdalne monitorowanie i informowanie o statusie serwera,
 - 3) szyfrowane połączenie oraz autentykację i autoryzację użytkownika,
 - 4) możliwość podmontowania zdalnych wirtualnych napędów,
 - 5) wirtualną konsolę z dostępem do myszy, klawiatury,
 - 6) wsparcie dla IPv6,
 - 7) wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH,
 - 8) integracja z Active Directory,
 - 9) wsparcie dla dynamic DNS.
14. System bezpieczeństwa serwera realizowany poprzez następujące zabezpieczenia:
 - 1) wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera;
 - 2) blokada zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych;
 - 3) moduł TPM 2.0.
15. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzanie serwerem klasy Microsoft Windows Server Standard 2025 wraz z 25 licencjami dostępowymi umożliwiającymi korzystanie przez 25 użytkowników z zasobów klastra serwerowego lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności. Oferowany system musi mieć możliwość zainstalowania co najmniej 1 wersji wstecz (tj. Windows Server 2022).

Warunki równoważności dla dostawy oprogramowania Microsoft Windows Server Standard 2025 wraz z 25 licencjami dostępowymi Microsoft Windows Server 2025 CAL User:

 - 1) 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 dla minimum 25 użytkowników.
 - 2) Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
 - 3) 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.
 - 4) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
 - 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
 - 6) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
 - 7) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
 - 8) Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;

- 9) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
 - 10) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
 - 11) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
 - 12) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
 - 13) Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
 - 14) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
 - 15) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
 - 16) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
 - 17) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
 - 18) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
 - 19) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
 - 20) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
16. 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.
17. Jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent serwera opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub ISO 14001 lub inny równoważny dokument poświadczający, że producent serwera posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany serwer 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 oświadczenia producenta serwera lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany serwer i jego/ich producenta/producentów wymagań w zakresie określonym powyżej.
18. Gwarancja: min. 60 miesięcy gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem naprawy do następnego dnia roboczego od przyjęcia zgłoszenia zgodnie z warunkami gwarancji producenta dla tego typu i rodzaju gwarancji, w przypadku awarii dysków Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość

fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji przez portal producenta serwera. Gwarancja powinna rozpocząć swój bieg od dnia podpisania końcowego protokołu odbioru całego zamówienia. Możliwość przedłużenia gwarancji do co najmniej 7 lat.

3.2.2. Zakup macierzy dyskowej SAN (1 szt.)

Minimalne parametry techniczne macierzy dyskowej SAN:

1. Obudowa typu RACK o wysokości maksymalnie 3U z możliwością instalacji do 24 dysków 2.5" Hot-Plug.
2. Macierz musi posiadać co najmniej 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe.
3. Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii.
4. Macierz musi mieć możliwość obsługi dysków SSD, SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS w obrębie macierzy dyskowej. Macierz musi obsługiwać dyski 2,5" i 3,5" (możliwe w ramach dołączonej półki). Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 100 dysków twardych.
5. Macierz musi posiadać co najmniej 4 porty FC 16 Gb/s (2 porty FC na kontroler). W zestawie niezbędne okablowanie do podłączenia macierzy z serwerami zapewniające możliwie najszybszy przesył danych oferowany przez porty wraz z wkładkami.
6. Zainstalowane min. 6 dysków Hot-Plug SAS o prędkości min. 12 Gb/s o pojemności co najmniej 1,2 TB każdy oraz 3 dyski twarde Hot-Plug SSD SAS o prędkości min. 12 Gb/s o pojemności co najmniej 1,9 TB każdy.
7. Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID5, RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping).
8. Macierz musi umożliwiać definiowanie globalnych dysków Hot-spare.
9. Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
10. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
11. Macierz musi umożliwiać dokonywanie na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.
12. Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.
13. Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na co najmniej 3 typach

- dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy.
14. Macierz musi umożliwiać jednocześnie podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).
 15. Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, VMWare.
 16. Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwóch niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
 17. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje Wykonawca jest je zobowiązany dostarczyć w ramach niniejszego postępowania.
 18. Jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent macierzy opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub ISO 14001 lub inny równoważny dokument poświadczający, że producent macierzy posiada system zarządzania energią, zmniejszający zużycie energii, wpływ na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowana macierz 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 oświadczenia producenta macierzy lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowaną macierz i jej producenta wymagań w zakresie określonym powyżej.
 19. Gwarancja: min. 60 miesięcy gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem naprawy do następnego dnia roboczego od przyjęcia zgłoszenia zgodnie z warunkami gwarancji producenta dla tego typu i rodzaju gwarancji, w przypadku awarii dysków Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji przez portal producenta serwera. Gwarancja powinna rozpocząć swój bieg od dnia podpisania końcowego protokołu odbioru całego zamówienia. Możliwość przedłużenia gwarancji do co najmniej 7 lat.

3.3. Zakup serwera (1 szt.).

Minimalne parametry techniczne serwera dla CUS:

1. Obudowa typu RACK o wysokości maksymalnie 1U z możliwością instalacji min. 8 dysków 2.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych.
2. Płyta główna z możliwością zainstalowania jednego procesora.
3. Zainstalowany jeden procesor klasy x86 dedykowany do pracy z oferowanym serwerem, umożliwiający osiągnięcie przez serwer wyniku co najmniej 110 punktów w teście SPECrate2017_fp_base według wyników publikowanych na stronie www.spec.org. Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie dla procesora dedykowanego do pracy z zaoferowanym serwerem żądanej przez Zamawiającego wydajności.
4. Pamięć RAM: zainstalowane min. 128 GB w najnowszej technologii oferowanej przez producenta, płyta główna musi obsługiwać do min. 128 GB pamięci RAM DDR5, minimum 4 sloty na pamięć w oferowanej konfiguracji obsadzone kośćmi pamięci.
5. Zabezpieczenia pamięci RAM: Memory Rank Sparing i/lub Memory Mirror i/lub Single Device Data Correction i/lub Memory Lockstep i/lub Chipkill i/lub Extended ECC i/lub Advanced Memory Device Correction i/lub AMD Memory Guard i/lub ECC i/lub Demand Scrubbing i/lub Patrol Scrubbing i/lub Permanent Fault Detection (PFD).
6. Zintegrowana karta graficzna ze złączem VGA.
7. Interfejsy sieciowe: Wbudowane co najmniej 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT, co najmniej 2 interfejsy w 10GbE w standardzie SFP+ z dedykowanymi wkładkami do każdego portu.
8. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 4 dyski twarde Hot-Plug SSD SATA o prędkości min. 6 Gb/s o pojemności co najmniej 960 GB każdy. W przypadku uszkodzenia dysku w okresie gwarancji Zamawiający wymaga by uszkodzony dysk pozostał jego własnością.
9. Kontroler RAID: Sprzętowy kontroler dyskowy umożliwiający konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60 i podtrzymaniem bateryjnym.
10. Wbudowane porty: min. 3 porty USB, w tym co najmniej 1 port USB musi być dostępny z przodu obudowy. Ilość dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęźniaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera.
11. Wentylatory: typu Hot Plug.
12. Zasilacze: typu Hot Plug o mocy nieprzekraczającej 1000 W każdy.
13. Karta/moduł zarządzania: Niezależny od zainstalowanego na serwerze systemu operacyjnego posiadający dedykowane złącze umożliwiający zdalne zarządzanie:
 - 1) zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
 - 2) zdalne monitorowanie i informowanie o statusie serwera,
 - 3) szyfrowane połączenie oraz autentykację i autoryzację użytkownika,
 - 4) możliwość podmontowania zdalnych wirtualnych napędów,
 - 5) wirtualną konsolę z dostępem do myszy, klawiatury,
 - 6) wsparcie dla IPv6,
 - 7) wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH,
 - 8) integracja z Active Directory,
 - 9) wsparcie dla dynamic DNS.
14. System bezpieczeństwa serwera realizowany poprzez następujące zabezpieczenia:

- 1) wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera;
 - 2) blokada zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych;
 - 3) moduł TPM 2.0.
15. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzanie serwerem klasy Microsoft Windows Serwer Standard 2025 wraz z 10 licencjami dostępowymi umożliwiającymi korzystanie przez 10 użytkowników z zasobów serwera lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności.
- Warunki równoważności dla dostawy oprogramowania Microsoft Windows Serwer Standard 2025 wraz z 10 licencjami dostępowymi Microsoft Windows Server 2025 CAL User:
- 1) 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 dla minimum 10 użytkowników.
 - 2) Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
 - 3) 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.
 - 4) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
 - 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
 - 6) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
 - 7) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
 - 8) Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
 - 9) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
 - 10) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
 - 11) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
 - 12) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
 - 13) Wbudowana zaporą internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
 - 14) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
 - 15) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
 - 16) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
 - 17) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

- 18) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
 - 19) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
 - 20) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
16. 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.
 17. Jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent serwera opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub ISO 14001 lub inny równoważny dokument poświadczający, że producent serwera posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany serwer 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 oświadczenia producenta serwera lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany serwer i jego/ich producenta/producentów wymagań w zakresie określonym powyżej.
 18. Gwarancja: min. 60 miesięcy gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem naprawy do następnego dnia roboczego od przyjęcia zgłoszenia zgodnie z warunkami gwarancji producenta dla tego typu i rodzaju gwarancji, w przypadku awarii dysków Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji przez portal producenta serwera. Gwarancja powinna rozpocząć swój bieg od dnia podpisania końcowego protokołu odbioru całego zamówienia. Możliwość przedłużenia gwarancji do co najmniej 7 lat.

3.4. Zakup przełącznika TYP A (3 szt.).

Aktualnie Zamawiający użytkuje urządzenia UTM firmy Fortinet Inc. (Urząd Gminy – urządzenie UTM Fortigate 60F; Centrum Usług Społecznych – urządzenie UTM Fortigate 40E) przedmiotem zamówienia jest dostawa urządzeń w postaci przełączników sieciowych TYP A i TYP B oraz urządzeń typu Access Point dla obu tych jednostek umożliwiających razem z istniejącymi urządzeniami UTM stworzyć jedną wspólną platformę bezpieczeństwa i kontroli ruchu sieciowego umożliwiającą centralne zarządzanie z jednej konsoli zarządzania z istniejącymi urządzeniami UTM w celu zapewnienia jednolitego i spójnego systemu bezpieczeństwa oraz polityk zarządzania ruchem w całej sieci. W przypadku jeżeli Wykonawca nie jest w stanie zaoferować rozwiązania kompatybilnego z istniejącymi urządzeniami UTM w celu zachowania zasady konkurencyjności Zamawiający dopuszcza dostawę całej platformy

bezpieczeństwa uwzględniającej wymianę urządzeń UTM na inne, które umożliwią integrację z oferowanymi przełącznikami sieciowymi oraz urządzeniami Acces Point uwzględniając minimalne kryteria równoważności dla urządzeń UTM określone w rozdziale 2 niniejszego dokumentu.

Minimalne parametry techniczne przełącznika TYP A:

1. Rodzaj urządzenia: zarządzany przełącznik L2.
2. Rodzaj obudowy: umożliwiający montaż w szafie RACK (wraz z kompletem szyn/wieszaków do montażu w szafie RACK).
3. Przepustowość routowania/przełączania: min. 175 Gbps.
4. Prędkość przekazywania: min. 250 Mpps.
5. Rozmiar tablicy MAC: min. 32 000 wpisów.
6. Bufor pamięci: min. 2 MB.
7. Pamięć RAM: min: 512 MB.
8. Pamięć flash min: 64 MB.
9. Dostępne interfejsy: min. 48 x RJ45 10/100/1000 Mbps; 4 x sloty SFP+ 10G. Dodatkowo w zestawie moduły światłowodowe SFP+ 10 Gbps (4 szt.) dedykowane do dostarczonego urządzenia lub zamienniki oraz patchcordsy światłowodowe SFP+ z wtyczkami i osłonkami o długości 3 m (4 szt.).
10. Obsługiwane standardy komunikacyjne: IEEE 802.1Q; IEEE 802.3ad; IEEE 802.1D; IEEE 802.1w; IEEE 802.1s; IEEE 802.1X, IEEE 802.1p.
11. Dodatkowo obsługa: QoS, VLAN, ACL, DHCP, IPv4, IPv6, Telnet, SNMP v1/v2c/v3, Http/Https, SSL, SSHv1/SSHv2, RADIUS/TACACS+.
12. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany przełącznik 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 przełącznika lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany przełącznik wymagań w zakresie określonym powyżej.
13. Przełączniki sieciowe muszą być objęte rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora w okresie do dnia 30.06.2026 r.
14. Co najmniej 24 miesiące gwarancji producenta.

3.5. Zakup przełącznika TYP B (1 szt.).

Aktualnie Zamawiający użytkuje urządzenia UTM firmy Fortinet Inc. (Urząd Gminy – urządzenie UTM Fortigate 60F; Centrum Usług Społecznych – urządzenie UTM Fortigate 40E) przedmiotem zamówienia jest dostawa urządzeń w postaci przełączników sieciowych TYP A i TYP B oraz urządzeń typu Access Point dla obu tych jednostek umożliwiających razem z istniejącymi urządzeniami UTM stworzyć jedną wspólną platformę bezpieczeństwa i kontroli ruchu sieciowego umożliwiającą centralne zarządzanie

z jednej konsoli zarządzania z istniejącymi urządzeniami UTM w celu zapewnienia jednolitego i spójnego systemu bezpieczeństwa oraz polityk zarządzania ruchem w całej sieci. W przypadku jeżeli Wykonawca nie jest w stanie zaoferować rozwiązania kompatybilnego z istniejącymi urządzeniami UTM w celu zachowania zasady konkurencyjności Zamawiający dopuszcza dostawę całej platformy bezpieczeństwa uwzględniającej wymianę urządzeń UTM na inne, które umożliwią integrację z oferowanymi przełącznikami sieciowymi oraz urządzeniami Acces Point uwzględniając minimalne kryteria równoważności dla urządzeń UTM określone w rozdziale 2 niniejszego dokumentu.

Minimalne parametry techniczne przełącznika TYP B:

1. Rodzaj urządzenia: zarządzany przełącznik L2/L3
2. Rodzaj obudowy: umożliwiający montaż w szafie RACK (wraz z kompletem szyn/wieszaków do montażu w szafie RACK).
3. Przepustowość routowania/przełączania: min. 14 Gbps.
4. Prędkość przekazywania: min. 20 Mpps.
5. Rozmiar tablicy MAC: min. 8 000 wpisów.
6. Dostępne interfejsy: min. 8 x RJ45 10/100/1000 Mbps, min. 2 porty SFP 1 GbE.
7. Obsługiwane standardy komunikacyjne: IEEE 802.1D, IEEE 802.1Q, IEEE 802.1ad, IEEE 802.1af, IEEE 802.1p, IEEE 802.1s, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.3u.
8. Dodatkowo obsługa: QoS, VLAN, ACL, DHCP, SNMP, Http/Https, SSL, SSH.
9. Obsługa PoE, min. 120 W.
10. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany przełącznik 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 przełącznika lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany przełącznik wymagań w zakresie określonym powyżej.
11. Co najmniej 24 miesiące gwarancji producenta.

3.6. Zakup NAS (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Obudowa wolnostojąca.
2. Procesor wielordzeniowy.
3. Pamięć RAM: min. 16 GB.
4. Oprogramowanie systemu operacyjnego umożliwiające minimum: zarządzanie i administrację urządzeniem, tworzenie kopii zapasowych z komputerów i serwerów z panelem zarządzania kopiami oraz ich przywracaniem, możliwością raportowania i powiadomień o wykonywaniu tych kopii, udostępnianie plików, zarządzanie przestrzenią dyskową, grupowanie dysków, zarządzanie dostępem i użytkownikami, wyszukiwanie plików, kompresowanie plików.
5. Możliwość zainstalowania łącznie 12 dysków 3,5-calowych.
6. Zainstalowane dyski: min. 5 x 12 TB, o prędkości 7200 RPM, dyski muszą być zgodne z urządzeniem NAS, tj. które znajdują się na liście zgodności prowadzonej przez producenta urządzenia NAS lub

które zostały przetestowane pod kątem zgodności z produktami producenta urządzenia NAS. Dyski muszą być przeznaczone do pracy ciągłej z deklarowanym przez producenta czasem pracy (MTBF) min. 2 000 000 h.

7. RAID 0, 1, 5, 6, 10.
8. Interfejsy sieciowe: 4 x Port Gigabit sieci Ethernet (RJ45) z obsługą funkcji Link Aggregation.
9. Porty USB: min. 2 x USB3.2.
10. 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. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany NAS wymagań w zakresie określonym powyżej.
11. Co najmniej 60 miesięcy gwarancji producenta na dyski oraz urządzenie główne w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dyski Zamawiający wymaga, aby dyski pozostały u Zamawiającego.

3.7. Zakup UPS TYP A (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Typ obudowy: RACK, max, 2U, Wykonawca jest zobowiązany dostarczyć szyny do montażu UPS w szafie RACK.
2. Moc pozorna: min. 3000 VA.
3. Moc rzeczywista: min. 2700 W.
4. Architektura UPSa: line-interactive lub online.
5. Typ przebiegu: sinusoidalny.
6. Liczba i rodzaj gniazdek z utrzymaniem zasilania: min. 8x IEC320 C13.
7. Typ gniazda wejściowego: C14 lub C20.
8. Czujnik temperatury.
9. Czas podtrzymania dla obciążenia 100%: min. 3 min.
10. Czas podtrzymania przy obciążeniu 50%: min. 10 min.
11. Zabezpieczenia: przeciwprzepięciowe, przeciwzwarceniowe, przeciwprzeciążeniowe.
12. Wyświetlacz LCD lub diody LED sygnalizujące stan pracy urządzenia oraz umożliwiające wyłączenie fizyczne urządzenia.
13. Alarmy dźwiękowe urządzenia sygnalizujące stan pracy urządzenia w zakresie określonych przez producenta zdarzeń.
14. Interfejsy: min. 1 x USB, 1 x RJ45, w zestawie karta zdalnego zarządzania UPS umożliwiającą zdalny monitoring oraz zarządzanie UPS przy wykorzystaniu przeglądarki internetowej.
15. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany UPS 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 UPS lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany UPS wymagań w zakresie określonym powyżej.

16. W zestawie dodatkowy moduł bateryjny kompatybilny z dostarczonym urządzeniem nieprzekraczający rozmiaru 2U wydłużający czas podtrzymania dla obciążenia 100 % do min. 10 min. łącznie z urządzeniem UPS.
17. Gwarancja producenta: min. 60 miesięcy gwarancji producenta na urządzenie oraz baterię.

3.8. Zakup UPS TYP B (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Typ obudowy: RACK, max, 2U, Wykonawca jest zobowiązany dostarczyć szyny do montażu UPS w szafie RACK.
2. Moc pozorna: min. 3000 VA.
3. Moc rzeczywista: min. 2200 W.
4. Architektura UPSa: line-interactive lub online.
5. Typ przebiegu: sinusoidalny.
6. Liczba i rodzaj gniazdek z utrzymaniem zasilania: min. 6x IEC320 C13.
7. Typ gniazda wejściowego: C14 lub C20.
8. Czas podtrzymania dla obciążenia 100%: min. 3 min.
9. Czas podtrzymania przy obciążeniu 50%: min. 10 min.
10. Zabezpieczenia: przeciwprzepięciowe, przeciwzwarceniowe, przeciwprzeciążeniowe.
11. Wyświetlacz LCD lub diody LED sygnalizujące stan pracy urządzenia oraz umożliwiające wyłączenie fizyczne urządzenia.
12. Alarmy dźwiękowe urządzenia sygnalizujące stan pracy urządzenia w zakresie określonych przez producenta zdarzeń.
13. Interfejsy: min. 1 x USB, 1 x RJ45, w zestawie karta zdalnego zarządzania UPS umożliwiającą zdalny monitoring oraz zarządzanie UPS przy wykorzystaniu przeglądarki internetowej.
14. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany UPS 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 UPS lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany UPS wymagań w zakresie określonym powyżej.
15. Gwarancja producenta: min. 60 miesięcy gwarancji producenta na urządzenie oraz baterię.

3.9. Zakup tokenu (5 szt.).

Minimalne parametry techniczne urządzenia:

1. Typ urządzenia: Token sprzętowy USB (urządzenie generujące jednorazowe hasła OTP - One-Time Password).
2. Przeznaczenie: Uwierzytelnianie dwuskładnikowe (2FA) w rozwiązaniach zabezpieczających, np. VPN, aplikacje webowe .
3. Współpraca z urządzeniami producenta FortiGate i systemami zabezpieczającymi tego producenta.
4. Wykorzystanie algorytmów kryptograficznych do generowania jednorazowych haseł.
5. Klucze uwierzytelniające muszą być przechowywane w urządzeniu.
6. Szyfrowanie: SHA-1, SHA-256, 128-bit AES, 192-bit AES, 256-bit AES.
7. Gwarancja producenta: min. 24 miesiące.

3.10. Zakup access point (2 szt.).

Aktualnie Zamawiający użytkuje urządzenia UTM firmy Fortinet Inc. (Urząd Gminy – urządzenie UTM Fortigate 60F; Centrum Usług Społecznych – urządzenie UTM Fortigate 40E) przedmiotem zamówienia jest dostawa urządzeń w postaci przełączników sieciowych TYP A i TYP B oraz urządzeń typu Access Point dla obu tych jednostek umożliwiających razem z istniejącymi urządzeniami UTM stworzyć jedną wspólną platformę bezpieczeństwa i kontroli ruchu sieciowego umożliwiającą centralne zarządzanie z jednej konsoli zarządzania z istniejącymi urządzeniami UTM w celu zapewnienia jednolitego i spójnego systemu bezpieczeństwa oraz polityk zarządzania ruchem w całej sieci. W przypadku jeżeli Wykonawca nie jest w stanie zaoferować rozwiązania kompatybilnego z istniejącymi urządzeniami UTM w celu zachowania zasady konkurencyjności Zamawiający dopuszcza dostawę całej platformy bezpieczeństwa uwzględniającej wymianę urządzeń UTM na inne, które umożliwią integrację z oferowanymi przełącznikami sieciowymi oraz urządzeniami Access Point uwzględniając minimalne kryteria równoważności dla urządzeń UTM określone w rozdziale 2 niniejszego dokumentu.

Minimalne parametry techniczne urządzenia Access Point:

1. Obudowa umożliwiająca montaż na ścianie lub na suficie.
2. Co najmniej dwie anteny dookólne, Zamawiający dopuszcza anteny wewnętrzne.
3. Standard komunikacji: Wi-Fi 6 802.11a/b/g/n/ac/ax.
4. Pracujący na trzech częstotliwościach 2,4 GHz; 5 GHz; 6 GHz.
5. Min. przepustowość na częstotliwości 2,4 GHz: min. 500 Mb/s.
6. Min. przepustowość na częstotliwości 5 GHz: min. 1 Gbps.
7. Min. przepustowość na częstotliwości 6 GHz: min. 2 Gbps.
8. Standardy komunikacyjne: IEEE 802.11a, IEEE 802.11ac, IEEE 802.11ax, IEEE 802.11b, IEEE 802.11e, IEEE 802.11g, IEEE 802.11h, IEEE 802.11i, IEEE 802.11j, IEEE 802.11k, IEEE 802.11n, IEEE 802.11r, IEEE 802.11v, IEEE 802.1x, IEEE 802.3ad, IEEE 802.3af, IEEE 802.3at, IEEE 802.3az, IEEE 802.3bz.
9. Funkcje: technologia MU-MIMO.
10. Gniazdo bezpieczeństwa zgodne z blokadą bezpieczeństwa Kensington. W zestawie zestaw do montażu.
11. Liczba klientów bezprzewodowych: min. 250.

12. Interfejsy urządzenia: min. 1 x 1000Base-T RJ45, min. 1 x USB.
13. Obsługiwane algorytmy szyfrujące: SSL, WPA, WPA2, WPA3.
14. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany Access Point 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 Access Point lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany AP wymagań w zakresie określonym powyżej.
15. Access pointy muszą być objęte rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora w okresie do dnia 30.06.2026 r.
16. Co najmniej 24 miesiące gwarancji producenta.

3.11. Zakup usług wdrożenia (1 szt.).

1. 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.
2. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
3. 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.

4. Opis przedmiotu zamówienia części nr 2.

4.1. Wymagania ogólne.

1. Dostarczone oprogramowanie musi być wolne od wad prawnych i fizycznych oraz nienoszące oznak użytkowania.
2. Dostarczone oprogramowanie musi być fabrycznie nowe, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego oprogramowania.
3. Niedopuszczalne są produkty prototypowe, oprogramowanie nie może 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. Wykonawca zapewni dostawę oprogramowania do wskazanej przez Zamawiającego lokalizacji.
5. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
6. 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.
7. 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.
8. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi”, „powinien”, „możliwość” określając w ten sposób wymaganą funkcjonalność oprogramowania.

4.2. Rozbudowa oprogramowania automatyzującego proces inwentaryzacji i monitorowania (1 szt.).

Przedmiotem zamówienia jest rozbudowa oprogramowania istniejącego w infrastrukturze Zamawiającego Axence nVision (moduły: Network, Inventory, DataGuard) poprzez podniesienie licencji do najwyższej aktualnej wersji oprogramowania oferowanej przez producenta oprogramowania na dzień składania oferty oraz zapewnienie możliwości wykorzystania oprogramowania dla 40 użytkowników do dnia 30.06.2026 r. lub dostawa równoważnej platformy oprogramowania zgodnie z kryteriami równoważności określonymi poniżej.

Minimalne wymagania funkcjonalne dla oprogramowania do zarządzania bezpieczeństwem IT oferowanego jako rozwiązanie równoważne:

1. Oprogramowanie musi składać się serwera zarządzającego, zdalnych konsoli oraz Agentów.
2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana powinna być przy użyciu szyfrowanego protokołu TLS 1.2.
3. Oprogramowanie musi umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych.
4. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych Administratorów - nadawanie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do grup urządzeń, jak i użytkowników.
5. Oprogramowanie musi posiadać funkcjonalność monitorowania infrastruktury serwerowej i sieciowej w zakresie:
 - a. wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping),
 - b. wizualizacji stanu urządzeń w postaci ikon urządzeń na mapach sieci,
 - c. wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie.
 - d. serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów,
 - e. serwerów pocztowych: - monitorowanie serwisu odbierającego, jak i wysyłającego pocztę, - możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), - możliwość wykonywania operacji testowych, - możliwość wysłania powiadomienia, jeśli serwer pocztowy nie działa,
 - f. monitorowania serwerów WWW i adresów URL,
 - g. obsługi szyfrowania SSL/TLS w powiadomieniach e-mail.
 - h. obsługi komunikatów syslog i pułapek SNMP.
 - i. monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych, - ruchu sieciowego, - podłączonych stacji roboczych- ruchu generowanego przez podłączone stacje robocze,
 - j. kontroli nad monitorem usług Windows,
 - k. monitorowania wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.
6. Oprogramowanie musi umożliwiać automatyczne gromadzenie danych o sprzęcie i oprogramowaniu na stacjach roboczych w zakresie:
 - a. informacji dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.;

- b. zestawienia posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade;
 - c. informacji o zainstalowanych aplikacjach oraz aktualizacjach Windows, umożliwiających audytowanie i weryfikację użytkownika licencji w organizacji;
 - d. informacji o wszystkich zmianach przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.;
 - e. możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiegokolwiek zmiany konfiguracji sprzętowej komputera;
 - f. możliwość odczytania numeru seryjnego (klucze licencyjne);
 - g. możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych;
 - h. możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
7. Oprogramowanie musi mieć możliwość prowadzenia bazy ewidencji majątku IT w zakresie:
- a. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji;
 - b. definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX, .PDF), skan dowolnego dokumentu, czy też własny komentarz, możliwość importu danych z zewnętrznego źródła np. (.CSV);
 - c. generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania;
 - d. archiwizacji i porównywania audytów środków trwałych;
 - e. tworzenia kodów kreskowych w Środkach Trwałych;
 - f. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy;
 - g. inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej co najmniej na system Android;
 - h. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji dodatkowego oprogramowania poprzez manualne wykonanie skanów inwentaryzacji offline).
8. Oprogramowanie musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:
- a. skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie, archiwów ZIP;
 - b. zarządzanie posiadanymi licencjami;
 - c. audyt legalności oprogramowania oraz powiadamianie w razie przekroczenia liczby posiadanych licencji;
 - d. zarządzanie posiadanymi licencjami: raport zgodności licencji;
 - e. możliwość przypisania do programów numerów seryjnych, wartości itp.

9. Oprogramowanie musi zapewniać integrację z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.
10. W zakresie kontroli dostępu do danych system musi umożliwiać:
 - a. automatyczne nadawanie użytkownikowi domyślnej polityki monitorowania i bezpieczeństwa;
 - b. ograniczenie ryzyka wycieku strategicznych danych za pośrednictwem przenośnych pamięci masowych oraz urządzeń mobilnych;
 - c. zabezpieczenie sieci firmowej przed wirusami instalującymi się automatycznie z pendrive'ów lub dysków zewnętrznych;
 - d. integracja z Windows Defender: zarządzanie ustawieniami wbudowanego antywirusa wraz z możliwością alarmowania o wykrytych problemach oraz wynikach skanowania;
 - e. integracja z Windows Firewall: włączanie i wyłączanie zapory dla wybranych typów połączeń, tworzenie reguł ruchu, odczyt stanu zapory na stacjach roboczych;
 - f. możliwość usuwania nieistniejących/zutylizowanych nośników danych (np. USB);
 - g. alarmy o podłączonym urządzeniu obcym (nieposiadającym atrybutu „nośnik zaufany”);
 - h. integracja z Windows Bitlocker: odczyt stanu modułu TPM oraz zaszyfrowania woluminów;
 - i. zdefiniowanie polityki przenoszenia danych firmowych przez pracowników wraz z odpowiednimi uprawnieniami;
 - j. informacje o urządzeniach podłączonych do danego komputera;
 - k. lista wszystkich urządzeń podłączonych do komputerów w sieci;
 - l. audyt (historia) połączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych;
 - m. zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników;
 - n. centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory.

Rozwiązania zastępujące dotychczas funkcjonujące u Zamawiającego Wykonawca dostarcza i wdraża na swój koszt. Wykonawca przeprowadzi instruktaże stanowiskowe i będzie świadczył asystę techniczną w zakresie umożliwiającym pracownikom jednostki Zamawiającego płynną obsługę wymienianego oprogramowania. Wdrożenie rozwiązania równoważnego nie może zakłócić bieżącej pracy Zamawiającego oraz musi zapewnić ciągłość pracy i musi odbywać się zgodnie z wytycznymi wynikającymi z rozdziału nr 4.1 niniejszego dokumentu.