|  |  |
| --- | --- |
| Numer sprawy: IOŚ.I.271.4.2024 | Kiwity, dnia 16.12.2024 |
| Gmina Kiwity  ul. Kiwity 28 11-106 Kiwity  Szczegółowy Opis Przedmiotu Zamówienia  na dostawę sprzętu informatycznego związana z realizacją projektu  „Cyberbezpieczny Samorząd” | |

Spis treści

[1. Zestawienie ilościowe. 3](#_Toc177501367)

[2. Wymagania ogólne w zakresie dostawy sprzętu i oprogramowania. 3](#_Toc177501368)

[3. Proces współpracy uruchomienia urządzenia backup. 4](#_Toc177501369)

[4. Zasada równoważności rozwiązań i neutralności technologicznej. 5](#_Toc177501370)

[5. Zakup urządzenia backup (1 szt.). 7](#_Toc177501371)

[6. Zakup serwera (1 szt.). 8](#_Toc177501372)

[7. Zakup UTM (1 szt.). 11](#_Toc177501373)

# Zestawienie ilościowe.

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa | Ilość |
| 1. | Zakup urządzenia backup | 1 szt. |
| 2. | Zakup serwera | 1 szt. |
| 3. | Zakup UTM | 1 szt. |

# Wymagania ogólne w zakresie dostawy sprzętu i oprogramowania.

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

# Proces współpracy uruchomienia urządzenia backup.

1. Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uruchomienia produkcyjnego urządzenie backup uwzględniając obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
2. opis koncepcji realizacji prac przy wykorzystaniu dostarczonego oprogramowania i sprzętu urządzenia backup. Wykonawca jest dodatkowo zobowiązany do wdrożenia sieci VLAN w istniejącą infrastrukturę Zamawiającego poprzez wykonanie minimum: planowanie topologii VLAN, określenie zakresu adresacji IP, przypisanie portów na switchach, routing między VLAN-ami,
3. scenariusze testowe, procedury oraz wzory raportów testów,
4. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
5. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
6. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
7. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 15 dni kalendarzowych od dnia zawarcia umowy,
8. Zamawiający w terminie nie dłuższym niż 7 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
9. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
10. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
11. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
12. zatwierdzony projekt techniczny wraz procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.
13. Wykonawca zrealizuje wdrożenie urządzenia backup zgodnie z zakresem prac i projektem technicznym.
14. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań. Wykonawca opracuje koncepcję backupu dla wdrożonej infrastruktury opierając się na będącym częścią infrastruktury sprzętowo-systemowej Zamawiającego systemie backup.
15. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
16. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery”. Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.

Instruktaże.

1. Instruktaże stanowiskowe będą prowadzone w języku polskim w siedzibie Zamawiającego i obejmą zakresem m.in.: użytkowane oprogramowanie; budowę, architekturę i konfigurację rozwiązania; administrowanie wdrożonym rozwiązaniem.
2. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.
3. Instruktaże powinny trwać minimum 16 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób (maksymalnie 4 osoby).
4. Zamawiający nie dopuszcza przeprowadzenia instruktaży w trybie zdalnym (online).
5. Administratorzy rozwiązania po zakończeniu Instruktaży stanowiskowych muszą w szczególności umieć wykonywać czynności administracyjne związane z obsługą, utrzymaniem i monitoringiem klastra HA i systemu backup, znać i umieć realizować procedury backupu. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem rozwiązania, a także sposoby ich przeciwdziałania, wykrywania i usuwania. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować wdrożone rozwiązanie, jak również znać jego wdrożoną konfigurację.

# Zasada równoważności rozwiązań i neutralności technologicznej.

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

# Zakup urządzenia backup (1 szt.).

Przedmiotem zamówienia jest dostawa systemu backup w postaci urządzenia typu all-in-one umożliwiającego:

1. Tworzenie pełnych, przyrostowych i różnicowych kopii zapasowych danych.
2. Automatyczne tworzenie kopii zapasowych zgodnie z harmonogramem.
3. Możliwość przywracania danych na poziomie plików, folderów oraz pełnych systemów.
4. Ochronę przed ransomware poprzez monitorowanie systemu oraz funkcję natychmiastowego przywracania danych.
5. Obsługę deduplikacji danych w celu optymalizacji wykorzystania przestrzeni dyskowej.
6. Zapewnienie wysokiej dostępności danych poprzez replikację.

Minimalne parametry techniczne systemu backup:

1. Obudowa typu RACK wraz z szynami umożliwiającymi montaż urządzenia w szafie RACK.
2. Urządzenie musi oferować przestrzeń min. 16 TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji.
3. Urządzenie musi posiadać minimum 2 porty RJ45 1GbE oraz 2 porty SFP+ 10GbE.
4. Urządzenie musi zapewniać wsparcie dla protokołów CIFS i NFS oraz deduplikacji na źródle.
5. Urządzenie musi zapewniać wsparcie dla systemów operacyjnych: min. Windows, Linux, macOS.
6. Urządzenie musi zapewniać zgodność z systemami plików: NTFS, FAT32, ext3, ext4, XFS.
7. Urządzenie musi zawierać mechanizmy integracyjne z systemami wirtualizacji (min. VMware, Hyper-V) w celu ochrony maszyn wirtualnych.
8. Dostarczone urządzenie musi umożliwiać dodatkową rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention). Urządzenie powinno obsługiwać integrację z chmurami takimi jak AWS, Azure, i Google Cloud.
9. Urządzenie powinno realizować deduplikację in-line oraz kompresję danych przed ich zapisem.
10. Urządzenie powinno być zarządzane przez GUI oraz CLI.
11. Urządzenie powinno wspierać RAID5.
12. Urządzenie powinno oferować funkcjonalność WORM.
13. Urządzenie powinno oferować funkcje typowe dla systemu Disaster Recovery i Business Continuity (BCDR).
14. Urządzenie powinno umożliwiać weryfikację danych oraz zautomatyzowane procesy usuwania przeterminowanych danych.
15. Urządzenie powinno obsługiwać replikację i możliwość podziału na logiczne części.
16. Urządzenie powinno posiadać możliwość skonfigurowania harmonogramu kopii zapasowych opartego na najlepszych praktykach (np. kopia pełna raz w tygodniu, przyrostowa codziennie).
17. Urządzenie powinno zapewniać przepustowość sieciową i wydajność urządzenia dostosowaną do obsługi środowiska bez negatywnego wpływu na codzienną pracę.
18. Urządzenie musi zapewniać szyfrowanie danych zarówno podczas tworzenia kopii zapasowych, jak i podczas ich przesyłania oraz przechowywania (AES-256).
19. Urządzenie musi zapewniać dwustopniową weryfikację dostępu do urządzenia i oprogramowania w celu dodatkowego zabezpieczenia.
20. Urządzenie musi być zgodne z wymogami RODO zapewniając odpowiednie zabezpieczenia danych osobowych oraz możliwość zarządzania danymi zgodnie z prawem.
21. Urządzenie powinno umożliwiać tworzenie, zarządzanie i odzyskiwanie kopii migawkowych.
22. Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway.
23. Wykonawca jest zobowiązany do instalacji i wdrożenia urządzenia w oparciu o wcześniej przygotowany projekt techniczny określony w rozdziale „Proces współpracy uruchomienia urządzenia backup.”
24. Wykonawca zapewni gwarancję urządzenia w okresie 24 miesięcy oraz zapewni wsparcie producenta w okresie do dnia 3.04.2026 r. obejmujące gwarancję aktualizacji oprogramowania do najnowszej wersji.

# Zakup serwera (1 szt.).

Minimalne parametry techniczne serwera:

1. Obudowa typu RACK o wysokości maksymalnie 1U z możliwością instalacji do 6 dysków 2.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
2. Płyta główna z możliwością zainstalowania jednego procesora.
3. Zainstalowany jeden procesor klasy x86 dedykowany do pracy z oferowanym serwerem, umożliwiające osiągnięcie przez serwer wyniku co najmniej 99 punktów w teście SPECrate2017\_fp\_base dla konfiguracji jednoprocesorowej według wyników publikowanych na stronie [www.spec.org](http://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.
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.
6. Zintegrowana karta graficzna ze złączem VGA.
7. Interfejsy sieciowe: Wbudowane co najmniej 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie w standardzie BaseT.
8. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 6 dysków twardych Hot-Plug SSD SATA o prędkości min. 6 Gb/s o pojemności co najmniej 960 6B każdy. W przypadku uszkodzenia dysku w okresie gwarancji Zamawiający wymaga by uszkodzony dysk pozostał jego własnością.
9. Możliwość zainstalowania co najmniej dwóch dysków M.2 SATA z możliwością konfiguracji RAID 1.
10. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w co najmniej dwa nośniki typu flash z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
11. Kontroler RAID: Sprzętowy kontroler dyskowy umożliwiający konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
12. Wsparcie dla dysków samoszyfrujących.
13. 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, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera.
14. Wentylatory: zapewniającą odpowiednie chłodzenie urządzenia.
15. Zasilacz o mocy nieprzekraczającej 1100 W.
16. Karta zarządzania: Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:
    1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
    2. zdalne monitorowanie i informowanie o statusie serwera,
    3. szyfrowane połączenie oraz autentykacje 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.
17. 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;
18. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzenie serwerem klasy Microsoft Windows Serwer Standard w najnowszej oferowanej wersji przez producenta na dzień składania ofert wraz z 20 licencjami dostępowymi umożliwiającymi korzystanie przez 20 użytkowników lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności.

Warunki równoważności dla dostawy oprogramowania Microsoft Windows Serwer Standard wraz z 20 licencjami dostępowymi Microsoft Windows Server 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 20 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 uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
  12. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
  13. Wbudowana zapora internetowa (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.

1. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
2. 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 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, ze 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; Certyfikat NIST SP 800-193 lub inny równoważny dokument potwierdzający, że serwer spełnia wymagania normy NIST SP 800-193 ochrony przed cyberatakami. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany serwer i jego/ich producenta/producentów w zakresie określonym powyżej.
3. Gwarancja: min. 60 miesięcy gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dyski 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.

# Zakup UTM (1 szt.).

Zamawiający w ramach działania przewiduje dostawę urządzenia UTM – kompleksowej platformy bezpieczeństwa wraz z subskrypcją. Subskrypcja musi umożliwić Zamawiającemu korzystanie z aktualnych baz funkcji ochronnych producenta i serwisów oraz obejmować kontrolę aplikacji, IPS, antywirus, antyspam, web filtering. W ramach przedmiotu zamówienia Wykonawca musi zapewnić także wsparcie techniczne, które może być tylko realizowane przez producenta, dystrybutora, bądź oficjalnego partnera dystrybutora. Subskrypcja dla urządzenia UTM obejmująca wszystkie wymagania wskazane powyżej musi być dostarczona na okres do dnia 3.04.2026 r.

Minimalne wymagania funkcjonalne urządzenia lub platformy bezpieczeństwa:

1. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.
2. System realizujący funkcję Firewall musi dawać możliwość pracy trybie routera z funkcją NAT.
3. System musi wspierać IPv4 oraz IPv6 w zakresie: firewall, ochrony w warstwie aplikacji, protokołów routingu dynamicznego.
4. Redundancja, monitoring i wykrywanie awarii:
   1. 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,
   2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych,
   3. Monitoring stanu realizowanych połączeń VPN.
5. Interfejsy: co najmniej 6 x Ethernet 10/100/1000.
6. Wbudowany dysk twardy: co najmniej 100 GB.
7. Wydajność:
   * Przepustowość firewall – co najmniej 10 Gbps,
   * Liczba równoległych sesji – co najmniej 1,5 mln.
   * Przepustowość IPS – co najmniej 1 Gbps.
   * Liczba jednoczesnych klientów SSL VPN – co najmniej 200.
8. 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.
9. 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.
10. Połączenia VPN:
    * System musi umożliwiać konfigurację połączeń typu IPSec VPN,
    * System musi umożliwiać konfigurację połączeń typu SSL VPN.
11. 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.
12. 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.
13. 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.
14. 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,
15. 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.
16. 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.
17. 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.
18. 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.
19. 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 do dnia 3.04.2026 r.
20. Wykonawca zapewni gwarancję producenta na dostarczane urządzenie na okres do dnia 3.04.2026 r.