|  |  |
| --- | --- |
| Numer sprawy: **ZP.272.01.2026** |  |
| Szczegółowy Opis Przedmiotu Zamówienia  na dostawę sprzętu i oprogramowania informatycznego związaną z realizacją grantu w ramach projektu „Cyberbezpieczny Samorząd” | |

Spis treści

[1. Zestawienie ilościowe. 3](#_Toc210373434)

[2. Zasada równoważności rozwiązań i neutralności technologicznej. 4](#_Toc210373435)

[3. Przedmiot zamówienia . 7](#_Toc210373436)

[3.1. Wymagania ogólne. 7](#_Toc210373437)

[3.2. Zakup serwera (1 szt.). 10](#_Toc210373438)

[3.3. Zakup macierzy (1 szt.). 13](#_Toc210373439)

[3.4. Zakup UPS (1 szt.). 15](#_Toc210373440)

[3.5. Zakup UTM (1 szt.). 16](#_Toc210373441)

# Zestawienie ilościowe.

Dostawa sprzętu i oprogramowania informatycznego.

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa | Ilość |
| 1. | Zakup serwera | 1 szt. |
| 2. | Zakup macierzy | 1 szt. |
| 3. | Zakup UPS | 1 szt. |
| 4. | Zakup UTM | 1 szt. |

# 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.

# Przedmiot zamówienia.

# 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 lokalizacji przez Zamawiającego.
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzeń do działania, pozwalające na rozpoczęcie pracy oraz dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania.
8. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
9. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
10. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
11. Dla dostaw sprzętu informatycznego z oprogramowaniem Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania (w tym systemu operacyjnego) nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania (faktury, rachunki) w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.
12. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia sprzętu i oprogramowania – wymagania minimalne:
13. Wykonawca przygotuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producentów wdrażanego sprzętu i oprogramowania po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uwzględniające obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
14. scenariusze testowe, procedury oraz wzory raportów testów,
15. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
16. opis koncepcji realizacji prac,
17. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
18. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
19. Wykonawca przekaże do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 10 dni kalendarzowych od dnia zawarcia umowy,
20. Zamawiający w terminie nie dłuższym niż 5 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
21. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
22. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
23. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
24. zatwierdzony projekt techniczny wraz procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.
25. Wykonawca zrealizuje wdrożenia i migracje zgodnie z zakresem prac i projektem technicznym.
26. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
27. 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.
28. 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.
29. Instruktaże w zakresie dostarczonego sprzętu i oprogramowania – wymagania minimalne.
30. 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.
31. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.
32. Instruktaże powinny trwać minimum 8 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób (maksymalnie 2 osoby).
33. Zamawiający dopuszcza przeprowadzenia instruktaży w trybie zdalnym (online).
34. Administratorzy rozwiązania po zakończeniu Instruktaży stanowiskowych muszą w szczególności umieć wykonywać czynności administracyjne, a także instalacji oprogramowania, 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.
35. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi”, „powinien”, „możliwość” określając w ten sposób wymaganą funkcjonalność oprogramowania.

# Zakup serwera (1 szt.).

Minimalne parametry techniczne serwera:

1. Obudowa typu RACK o wysokości maksymalnie 2U z możliwością instalacji min. 12 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 dwóch procesorów.
3. Zainstalowane dwa procesory klasy x86 dedykowane do pracy z oferowanym serwerem, umożliwiające osiągnięcie przez serwer wyniku co najmniej 245 punktów w teście SPECrate2017\_fp\_base dla konfiguracji dwuprocesorowej 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. 256 GB w najnowszej technologii oferowanej przez producenta, płyta główna musi obsługiwać do min. 1 TB pamięci RAM DDR5, co najmniej 12 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 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT, co najmniej 2 interfejsy sieciowe 10Gb Ethernet w standardzie 10GBase-T, 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 2 dyski twarde Hot-Plug SSD SATA o prędkości min. 6 Gb/s o pojemności co najmniej 480 GB każdy oraz 5 dysków twardych Hot-Plug SAS o prędkości min. 12 Gb/s o pojemności co najmniej 2,4 TB 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.
10. Wsparcie dla dysków samoszyfrujących.
11. 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.
12. Wentylatory: typu Hot Plug.
13. Zasilacze: Redundantne typu Hot Plug o mocy nieprzekraczającej 700 W każdy.
14. 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 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.
15. 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.
16. Serwer powinien posiadać funkcjonalność umożliwiającą konfigurację i monitoring kluczowych komponentów (takich jak CPU, RAM, dyski, temperatury, statusy wentylatorów) za pomocą aplikacji mobilnej. Aplikacja powinna być dostępna na urządzenia mobilne działające na systemach Android oraz iOS i umożliwiać dostęp do serwera za pomocą popularnych protokołów bezprzewodowych, takich jak BLE lub Wi-Fi.
17. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzenie serwerem klasy Microsoft Windows Serwer Standard 2025 wraz z 20 licencjami dostępowymi umożliwiającymi korzystanie przez 20 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 20 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 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 2022, Microsoft Windows Server 2025.
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 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, 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. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany serwer i jego/ich producenta/producentów wymagań 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 dysków Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii w języku polskim poprzez ogólnopolską linię telefoniczną producenta oraz dedykowany portal techniczny producenta, dla obu kanałów w trybie ciągłym, tj. niezależnie od pory dnia, dni roboczych i dni wolnych od pracy. Zamawiający wymaga pojedynczego serwisowego punktu kontaktu dla całego rozwiązania Producenta (w tym także zaoferowanego oprogramowania) umożliwiającego komunikację w języku polskim. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocenę bezpieczeństwa cybernetycznego. Wszelkie naprawy mogą być realizowane przez osoby certyfikowane przez producenta, które po diagnostyce muszą z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) rozpocząć naprawę w siedzibie Zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. W przypadku jeżeli serwis gwarancyjny urządzeń nie będzie realizowany bezpośrednio przez producenta urządzenia, wówczas firma serwisująca musi posiadać certyfikat ISO 9001 oraz ISO 27001 lub inny równoważny dokument poświadczający, że usługi serwisu świadczone będą zgodnie z zasadami wynikającymi z tych norm oraz firma serwisująca musi posiadać autoryzacje producenta urządzeń, w takim przypadku Wykonawca jest zobowiązany dostarczyć wraz z ofertą dokumenty potwierdzające spełnienie przez firmę serwisującą przedmiotowego wymogu. Możliwość przedłużenia gwarancji producenta do 72 miesięcy.

# Zakup macierzy (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Obudowa typu RACK o wysokości maksymalnie 3U z możliwością instalacji do 24 dysków 2.5" Hot-Plug z blokadą służącą do ochrony nieautoryzowanego dostępu do dysków twardych.
2. Macierz musi posiadać co najmniej 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
3. Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.
4. Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” i 3,5”. Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 100 dysków twardych.
5. Macierz musi posiadać co najmniej 8 portów iSCSI SFP+/SFP28 25Gb/s (4 porty na kontroler). Należy również dostarczyć min. 8 sztuk przewodów iSCSI SFP+/SFP28 25Gb/s kompatybilnych z urządzeniem dedykowane przez producenta rozwiązania o długości minimum 2 m.
6. Zainstalowane min. 5 dysków Hot-Plug SAS SSD o prędkości min. 24 Gb/s o pojemności co najmniej 1,92 TB każdy skonfigurowane w RAID5 oraz min. 8 dysków Hot-Plug SAS o prędkości min. 12 Gb/s o pojemności co najmniej 2,4 TB każdy skonfigurowane w RAID5
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 oraz dedykowanie dysków Hot-spare do konkretnych grup RAID.
9. Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
10. Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).
11. Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.
12. 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.
13. Macierz musi umożliwiać dokonywania 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.
14. Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.
15. 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.
16. Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).
17. Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, VMWare.
18. 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 dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
19. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje Wykonawca jest je zobowiązany dostarczyć w ramach niniejszego postępowania.
20. 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, wpływy na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, ze 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.
21. Gwarancja: min. 60 miesięcy gwarancji producenta obejmująca wszystkie komponenty macierzy wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dysków Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii w języku polskim poprzez ogólnopolską linię telefoniczną producenta oraz dedykowany portal techniczny producenta, dla obu kanałów w trybie ciągłym, tj. niezależnie od pory dnia, dni roboczych i dni wolnych od pracy. Zamawiający wymaga pojedynczego serwisowego punktu kontaktu dla całego rozwiązania Producenta (w tym także zaoferowanego oprogramowania) umożliwiającego komunikację w języku polskim. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocenę bezpieczeństwa cybernetycznego. Wszelkie naprawy mogą być realizowane przez osoby certyfikowane przez producenta, które po diagnostyce muszą z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) rozpocząć naprawę w siedzibie Zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. W przypadku jeżeli serwis gwarancyjny urządzeń nie będzie realizowany bezpośrednio przez producenta urządzenia, wówczas firma serwisująca musi posiadać certyfikat ISO 9001 oraz ISO 27001 lub inny równoważny dokument poświadczający, że usługi serwisu świadczone będą zgodnie z zasadami wynikającymi z tych norm oraz firma serwisująca musi posiadać autoryzacje producenta urządzeń, w takim przypadku Wykonawca jest zobowiązany dostarczyć wraz z ofertą dokumenty potwierdzające spełnienie przez firmę serwisującą przedmiotowego wymogu. Możliwość przedłużenia gwarancji producenta do 72 miesięcy.

# Zakup UPS (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Typ obudowy: umożliwiająca umieszczenie w szafie RACK a także zapewniająca ustawienie wolnostojące.
2. Moc pozorna: min. 3000 VA.
3. Moc rzeczywista: min. 3000 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. Czas podtrzymania dla obciążenia 100%: min. 3 min.
9. Czas podtrzymania przy obciążeniu 50%: min. 10 min.
10. Zabezpieczenia: przeciwprzepięciowe, przeciwzwarciowe, przeciwprzeciążeniowe.
11. Wyświetlacz LCD lub diody LED sygnalizujące stan pracy urządzenia.
12. Alarmy dźwiękowe urządzenia sygnalizujące stan pracy urządzenia w zakresie określonych przez producenta zdarzeń.
13. Interfejsy: min. 1 x USB, 1 x RJ45.
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. 24 miesiące.

# Zakup UTM (1 szt.).

W ramach działania przewiduje się zakup urządzenia UTM wraz z licencjami subskrypcyjnymi dla Urzędu Gminy w Siemieniu. 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 30.06.2026 r. niezależnie od oferowanych modeli licencjonowania producenta.

Minimalne wymagania techniczne urządzenia:

1. Przepustowość Firewall: min. 28 Gbps.
2. Musi obsługiwać min. 3 miliony jednoczesnych połączeń.
3. Musi obsługiwać co najmniej 200 połączeń VPN.
4. Wydajność IPsec VPN min. 25 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2 Gbps.
8. Automatyczna aktualizacja plików sygnatur antywirusowych.
9. Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji.
10. Możliwość wsparcia IPS z poziomu urządzenia poprzez dodatkowe subskrypcje.
11. Automatyczna aktualizacja sygnatur IPS.
12. IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy.
13. Wsparcie dla wszystkich głównych protokołów: HTTP, FTP, SMTP, POP3.
14. Ilość interfejsów sieciowych: minimum 8 portów Gigabit Ethernet RJ-45, min. 2 porty 10 GE SFP+.
15. Inne interfejsy: min. 1 port USB.
16. Wbudowany fabrycznie dysk twardy SSD o pojemności min. 100 GB.
17. Wsparcie VLAN: Musi posiadać minimum 200 sieci VLAN.
18. Administracja urządzenia musi być możliwa poprzez graficzny interfejs zarządzania.
19. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
20. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
21. Kontrola Aplikacji.
22. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
23. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS oparta o mechanizmy sztucznej inteligencji.
24. Ochrona przed atakami - Intrusion Prevention System.
25. Kontrola stron WWW.
26. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
27. Zarządzanie pasmem (QoS, Traffic shaping).
28. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
29. Analiza ruchu szyfrowanego protokołem SSL.
30. Analiza ruchu szyfrowanego protokołem SSH.
31. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN.
32. Zapewnienie obsługi Routingu statycznego, Policy Based Routingu, protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
33. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
34. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
35. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
36. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
37. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
38. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
39. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
40. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
41. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
42. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
43. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
44. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
45. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
46. Rozwiązanie powinno umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
47. Urządzenie powinno mieć możliwość generowania raportów.
48. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
49. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
50. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
51. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
52. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
53. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
54. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować następujące elementy: Kontrola Aplikacji, IPS, Antywirus, Antyspam, Antymalware, Web Filtering w okresie do dnia 30.06.2026 r.
55. Gwarancja producenta do dnia 30.06.2026 r. Gwarancja powinna obejmować również możliwość wymiany urządzenia na nowe w przypadku wady urządzenia UTM.