Załącznik nr 1

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Dostawa sprzętu komputerowego oraz wdrożenie systemów

 i rozwiązań teleinformatycznych w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU

 działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia

dotycząca realizacji projektu grantowego

„Cyfrowa Gmina”

**Część I**

Dostawa sprzętu komputerowego na potrzeby JST

**Część II**

Rozbudowa i modernizacja platform serwerowych oraz systemu składowania i archiwizacji danych

**Część III**

Rozbudowa i modernizacja sieci LAN oraz serwerowni

Opis przedmiotu zamówienia wg Wspólnego Słownika Zamówień (CPV):

30200000-1 Urządzenia komputerowe

30213000-5 Komputery osobiste

48620000-0 Systemy operacyjne

48000000-8 Pakiety oprogramowania i systemy informatyczne

48710000-8 Pakiety oprogramowania do kopii zapasowych i odzyskiwania

48820000-2 Serwery

48821000-9 Serwery sieciowe

48823000-3 Serwery plików

51610000-1 Usługi instalowania urządzeń komputerowych i przetwarzania informacji

72265000-0 Usługi konfiguracji oprogramowania

32428000-9 Modernizacja sieci

72800000-8  Usługi audytu komputerowego i testowania komputerów

**Część I**

Zawartość:

1. Ogólny opis przedmiotu zamówienia i wymagań Zamawiającego
2. Szczegółowe właściwości i wymagania funkcjonalno-użytkowe
3. Dostawa sprzętu komputerowego na potrzeby JST
4. System do komunikacji on-line oraz wideokonferencji
5. Warunki uruchomienia i odbioru wdrożonych rozwiązań oraz przekazania do eksploatacji

**Część II**

Zawartość:

1. Ogólny opis przedmiotu zamówienia i wymagań Zamawiającego
2. Szczegółowe właściwości i wymagania funkcjonalno-użytkowe
3. Rozbudowa i modernizacja platform serwerowych wraz z oprogramowaniem systemowym
4. Rozbudowa i modernizacja systemu składowania i archiwizacji danych oraz wykonywania kopii zapasowych posiadanej macierzy dyskowej
5. Warunki uruchomienia i odbioru wdrożonych rozwiązań oraz przekazania do eksploatacji

**Część III**

Zawartość:

1. Ogólny opis przedmiotu zamówienia i wymagań Zamawiającego
2. Szczegółowe właściwości i wymagania funkcjonalno-użytkowe
3. Rozbudowa i modernizacja sieci LAN, doposażenie serwerowni
4. System zapewnienia bezpieczeństwa teleinformatycznego (cyberbezpieczeństwo)
5. Warunki uruchomienia i odbioru wdrożonych rozwiązań oraz przekazania do eksploatacji

 **Część I**

1. **OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA I WYMAGAŃ ZAMAWIAJĄCEGO**
2. **Zakres przedmiotu zamówienia**

Przedmiotem zamówienia jest dostawa sprzętu komputerowego i innych urządzeń stanowiących elementy systemu komunikacji on-line oraz wideokonferencji, mająca na celu podniesienie poziomu cyfryzacji Jednostki w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego **„Cyfrowa Gmina”** o numerze POPC.05.01.00-00-0001/21-00

**Szczegółowy zakres zamówienia składa się z następujących zadań:**

1. Dostawa sprzętu komputerowego na potrzeby JST
	* + Komputer stacjonarny – 20 kpl.
		+ Monitor - 20 szt.
		+ Notebook - 10 szt.
		+ Oprogramowanie - pakiet zintegrowanych aplikacji biurowych – 30 kpl.
2. System do komunikacji on-line oraz wideokonferencji
* Komputer MiniPC – 1 szt.
* TV 49'' 4K Ultra HD -1 szt.
* Mobilny stojak do TV – 1 szt.
* Zestaw głośnomówiący – 2 szt.
* Kamera 4K – 2 szt.

**2. Ogólne wymagania Zamawiającego**

Zamawiający dopuszcza rozwiązania równoważne w przypadku wskazania w opisie przedmiotu zamówienia norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy PZP.

- W przypadku podania przez Zamawiającego nazw materiałów, producentów czy znaków towarowych należy je traktować jako przykładowe, mające na celu doprecyzowanie przedmiotu zamówienia oraz określające standard techniczny i jakościowy. Zamawiający, wskazując oznaczenie konkretnego producenta lub konkretny produkt przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty i rozwiązania równoważne o nie gorszych parametrach jakościowych, technicznych, eksploatacyjnych i użytkowych. Ciężar wykazania spełnienia tych wymagań leży po stronie wykonawcy w składanej ofercie lub jeżeli ten przypadek ma miejsce w trakcie realizacji umowy – w chwili zaistnienia konieczności dokonania takiej zmiany.

- W przypadku zastosowania zasad wskazanych powyżej w trakcie realizacji umowy, mogą one wystąpić pod warunkiem, że zmiany te nie będą wpływać na oferowany w ofercie przedmiot zamówienia i efekt zakreślony niniejszym OPZ.

- W przypadku zastosowania materiałów, urządzeń, wyrobów lub rozwiązań równoważnych, Wykonawca zobowiązany jest do ich wskazania w ofercie oraz do złożenia wraz z ofertą kart technicznych lub innych dokumentów potwierdzających, że oferowane rozwiązania równoważne spełniają wymagania Zamawiającego opisane w przedmiocie zamówienia.

**Wymagania ogólne dotyczące sprzętu:**

1. Wszystkie dostarczone urządzenia muszą być fabrycznie nowe, bez wad i uszkodzeń, nieregenerowane, nieużywane i nie będące przedmiotem wystaw i prezentacji oraz o ile nie wyspecyfikowano inaczej w wymaganiach szczegółowych dla urządzeń, wyprodukowane nie wcześniej niż 2021 roku.
2. Wszystkie urządzenia będą pochodziły z oficjalnego, europejskiego kanału dystrybucji.
3. Urządzenia zostaną dostarczone przez Wykonawcę własnym transportem i na własny koszt w miejsce wskazane przez Zamawiającego. Wszystkie urządzenia muszą być dostarczone w oryginalnych opakowaniach producenta.
4. Wszystkie urządzenia powinny być zgodne z normami UE i przeznaczone na rynek UE, oraz powinny posiadać certyfikat CE.
5. Dostarczany sprzęt powinien być kompletny i gotowy do uruchomienia, tak aby nie był konieczny zakup dodatkowych elementów czy akcesoriów.
6. Wykonawca dostarczy stosowne potwierdzenie gwarancji sprzętu i oprogramowania zapewniające, że sprzęt objęty jest gwarancją producenta.
7. Serwis sprzętu będzie świadczony przez producenta lub jego autoryzowanego partnera serwisowego posiadającego wdrożoną normę min. PN-EN ISO 9001 lub równoważną.
8. Sprzęt dostarczany w ramach niniejszego zamówienia, powinien być objęty 3 letnią gwarancją i wsparciem producenta, chyba że okres i warunki gwarancji zostały dodatkowo określony w opisie szczegółowym specyfikowanego wyposażenia/sprzętu.
9. Udzielona gwarancja producenta nie wyłącza uprawnień Zamawiającego z tytułu rękojmi w stosunku do Wykonawcy.

**Wymagania ogólne dotyczące oprogramowania:**

Wykonawca zobowiązany jest dostarczyć Zamawiającemu:

1. certyfikaty licencyjne wystawione przez producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na dedykowanym portalu klienckim;
2. nośniki instalacyjne Oprogramowania, o ile nie są dostępne w formie elektronicznej na dedykowanym portalu klienckim;
3. adresy poczty elektronicznej, numery telefonów oraz inne dane dostępowe umożliwiające Zamawiającemu korzystanie ze Wsparcia technicznego świadczonego przez producenta Oprogramowania w pełnym zakresie, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
4. zestawienie dostarczonych Zamawiającemu pozycji w zakresie Oprogramowania, zawierające m.in.: numer partii (SKU), pełna nazwa produktu, wersja i edycja oprogramowania, metryka licencyjna, rodzaj licencji (terminowa/bezterminowa), okres obowiązywania licencji, okres obowiązywania wsparcia technicznego, poziom wsparcia technicznego;
5. standardowe warunki licencyjne producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
6. standardowe warunki Wsparcia technicznego producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;
7. oświadczenie producenta Oprogramowania potwierdzające dostawę licencji i objęcie ich wsparciem technicznym na poziomie zgodnym z wymaganiami Zamawiającego, o ile nie potwierdzają jej certyfikaty licencyjne i standardowe warunki Wsparcia technicznego.

Realizacja powyższego zakresu zamówienia musi być wykonana w oparciu o obowiązujące przepisy, przez Wykonawcę posiadającego stosowne doświadczenie, uprawnienia i potencjał wykonawczy oraz osoby o odpowiednich kwalifikacjach i doświadczeniu zawodowym.

1. **SZCZEGÓŁOWE WŁAŚCIWOŚCI I WYMAGANIA FUNKCJONALNO - UŻYTKOWE**

**1. Dostawa sprzętu komputerowego na potrzeby JST**

**1.1. Komputer stacjonarny – 20 kpl.**

|  |  |
| --- | --- |
| **Parametr lub warunek** | **Minimalne wymagania** |
| Typ | Komputer stacjonarny przeznaczony do obsługi aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej i systemów dziedzinowych. W ofercie należy podać nazwę producenta, typ, model oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. |
| Obudowa | Typu Small Form Factor z obsługą kart PCI Express o niskim profilu:* 1 x PCI Express 3.0 x16,
* 1 x PCI Express 3.0 x1,

Umożliwiająca montaż min: 1 szt. na napęd optyczny 5,25” (dopuszcza się napędy typu wersji SLIM), oraz 1 szt. dysków 2,5”3.5”.Obudowa musi umożliwiać beznarzędziowe otwarcie, demontaż dysku M.2, napędu optycznego oraz kart rozszerzeń. Obudowa musi być wyposażona w czujnik otwarciaWbudowany głośnik o mocy min. 1W |
| Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera. Płyta główna wyposażona w min. 2 złącza M.2, w tym min. 1 dedykowane dla dysku SSD PCIe. |
| Procesor | Procesor klasy x86, zaprojektowany do pracy w komputerach stacjonarnych o wydajności nie mniejszej niż 14000 punktów na podstawie PerformanceTest w teście PASSMARK CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net na dzień składania ofert. Wynik oferowanego procesora w teście PASSMARK CPU Mark należy załączyć do oferty. |
| Pamięć operacyjna | 8GB GB, 3200MHz DDR4, 2 sloty na pamięć, z czego min. 1 wolny.Możliwość pracy pamięci w trybie dual channel. Możliwość rozbudowy do 64GB pamięci RAM |
| Dysk twardy | Min 512GB M.2 PCIe, wspierający sprzętowe szyfrowanie dysku, zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.  |
| Napęd optyczny | Nagrywarka DVD +/-RW wyposażona w tackę z zaczepami umożliwiającymi pracę w poziomie i pionie |
| Karta graficzna | Zintegrowana z procesorem |
| Audio | Zintegrowana karta dźwiękowa, zgodna z High Definition |
| Sieć | Zintegrowana karta LAN 100/1000Mbps |
| Porty/złącza | Wbudowane porty: * 1 x HDMI 2.1,
* 1 x DP 1.4,
* 7 x USB w tym min.: 3x USB 3.2 z przodu

obudowy (min. 1x USB-C), 4 x USB z tyłu obudowy, w tym min. 2 x USB 3.2; * port sieciowy RJ-45,
* porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy
* czytnik kart pamięci 7 w 1

Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. |
| Klawiatura/mysz | Klawiatura w układzie US USB + mysz z rolką USB |
| Zasilacz | Energooszczędny zasilacz o mocy nie większej niż 200W oraz sprawności na poziomie min. 85% posiadający certyfikat 80 PLUS.  |
| System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
	1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
	2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych
2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego
3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim
4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.
5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe
6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim
9. Wbudowany system pomocy w języku polskim.
10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.
16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.
18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."
24. Wbudowany mechanizm wirtualizacji typu hypervisor."
25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.
26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób, aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.
30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.
31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM
33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.
34. Możliwość tworzenia wirtualnych kart inteligentnych.
35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)
36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.
37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
38. Mechanizmy logowania w oparciu o:
	1. Login i hasło,
	2. Karty inteligentne i certyfikaty (smartcard),
	3. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
	4. Certyfikat/Klucz i PIN
	5. Certyfikat/Klucz i uwierzytelnienie biometryczne
39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5
40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.
41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach
42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń
43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
 |
| BIOS  | Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:* modelu komputera,
* numerze seryjnym,
* numerze inwentarzowym,
* MAC Adres karty sieciowej,
* wersja Biosu wraz z datą produkcji,
* zainstalowanym procesorze, jego taktowaniu i ilości rdzeni
* ilości pamięci RAM wraz z taktowaniem,
* stanie pracy wentylatora na procesorze
* stanie pracy wentylatora w obudowie komputera
* napędach lub dyskach podłączonych do portów SATA (model dysku twardego i napędu optycznego)

Możliwość z poziomu Bios:* wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy
* wyłączenia selektywnego (pojedynczego) portów SATA,
* wyłączenia karty sieciowej, karty audio, portu szeregowego,
* możliwość ustawienia portów USB w jednym z dwóch trybów:
1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer, ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB
2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej
* ustawienia hasła: administratora, Power-On, HDD,
* blokady aktualizacji BIOS bez podania hasła administratora
* wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów
* ostrzegania o zmianie konfiguracji sprzętowej komputera
* załadowania optymalnych ustawień Bios

- możliwość ustawienia polityki dotyczącej haseł (długość i trudność hasła)- możliwość włączenia/wyłączenia Device Guard- możliwość włączenia/wyłączenia uruchomienia komputera za pomocą kombinacji klawiszy na podłączonej klawiaturze |
| Zintegrowany System Diagnostyczny | Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów:* wykonanie testu pamięci RAM
* test dysku twardego
* test monitora
* test magistrali PCI-e
* test portów USB
* test płyty głównej
* test procesora

Wizualna lub dźwiękowa sygnalizacja w przypadku uszkodzenia bądź błędów któregokolwiek z powyższych podzespołów komputera.Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie:* PC: Producent, model
* BIOS: Wersja oraz data wydania Bios
* Procesor: Nazwa, taktowanie
* Pamięć RAM: Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci
* Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy
* Monitor: producent, model, rozdzielczość

System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera. |
| Certyfikaty i standardy | * Certyfikat ISO9001 lub równoważny dla producenta sprzętu **(należy załączyć do oferty)**
* Deklaracja zgodności CE dla urządzenia **(należy załączyć do oferty)**
* Certyfikat lub inny dokument potwierdzający poprawną współpracę z zaoferowanym systemem operacyjnym **(należy załączyć do oferty)**
* Certyfikat ISO14001 lub równoważny dla producenta sprzętu (należy załączyć na etapie dostawy )
* Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (należy załączyć na etapie dostawy )
 |
| Bezpieczeństwo | * Moduł TPM 2.0
 |
| Gwarancja | * 3 lata świadczona w miejscu użytkowania sprzętu (on-site)
* W przypadku awarii dysku twardego dysk uszkodzony pozostaje u Zamawiającego.
 |
| Wsparcie techniczne producenta | * możliwość weryfikacji u producenta konfiguracji fabrycznej i oferowanej zakupionego sprzętu
* możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji
* możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego
* naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub autoryzowanego partnera serwisowego producenta.
 |

**1.2. Monitor – 20 szt.**

|  |  |
| --- | --- |
| **Parametr lub warunek** | **Minimalne wymagania** |
| Ekran | Matowy 23.8'' AMVA 16:9 z podświetlaniem LED |
| Obszar widzialny | w pionie min. 296 mm, w poziomie min. 527 mm |
| Plamka matrycy | 0.275 mm  |
| Rozdzielczość | 1920 x 1080 (FHD 1080)  |
| Czas reakcji matrycy |  Max.4 ms  |
| Parametry obrazu  | jasność 250 cd/m², kontrast statyczny3 000:1 |
| Częstotliwość odświeżania | w poziomie 30 kHz - 80 kHz, w pionie 55 Hz - 75 Hz |
| Kąty widzenia  | poziomy i pionowy 178 °  |
| Gniazda we/wy | 1x 3,5 mm minijack, 1x 15-pin D-Sub, 1x HDMI, 1x DisplayPort, 3x USB 2.0  |
| Wbudowane głośniki | Tak  |
| Certyfikaty | * Certyfikat ISO9001 lub równoważny dla producenta sprzętu **(należy załączyć do oferty)**
* Deklaracja zgodności CE **(należy załączyć do oferty)**
* Certyfikaty - TCO min.5.0 , EnergyStar min.5.0 (należy załączyć na etapie dostawy )
 |
| Standard VESA | 100 x 100  |
| Akcesoria w zestawie |  Kabel zasilający, Kabel HDMI, Podstawa regulowana |
| Gwarancja | 3 lata świadczona w miejscu użytkowania sprzętu (on-site) |

**1.3. Notebook - 10 szt.**

|  |  |
| --- | --- |
| **Parametr lub warunek** | **Minimalne wymagania** |
| Typ | Komputer przenośny przeznaczony do obsługi aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej i systemów dziedzinowych. W ofercie należy podać nazwę producenta, typ, model oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. |
| Ekran | Matowy, matryca TFT 15.6” w technologii IPS/PLS/WVA, z podświetleniem w technologii LED, rozdzielczość FHD 1920x1080, jasność 300nits, kontrast 800:1, Kąt otwarcia pokrywy ekranu min.180 stopni. |
| Procesor | Procesor klasy x86, zaprojektowany do pracy w komputerach przenośnych o wydajności nie mniejszej niż 13500 punktów na podstawie PerformanceTest w teście PASSMARK CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net na dzień składania ofert. Wynik oferowanego procesora w teście PASSMARK CPU Mark należy załączyć do oferty  |
| Pamięć operacyjna | 16GB GB, 3200MHz DDR4, min. 1 wolny slot.Możliwość pracy pamięci w trybie dual channel. Możliwość rozbudowy do 40GB pamięci RAM |
| Dysk twardy | Min 512GB M.2 PCIe, zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. Możliwość rozbudowy do konfiguracji dwudyskowej przez dostępny wbudowany drugi slot M.2 do obsługi dysków |
| Karta graficzna | Zintegrowana z procesorem. |
| Audio | * Zintegrowana karta dźwiękowa, zgodna z High Definition.
* Wbudowane w obudowie komputera: głośniki Dolby Audio stereo (2x2W),
* Wbudowane dwa mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute)
* Wbudowana kamera video 720p z mechaniczną zasłoną obiektywu
 |
| Sieć | Wbudowane karty sieciowe WLAN w standardzie 802.11AX 2x2, LAN 100/1000 Mbps, Bluetooth 5.1  |
| Porty/złącza | Wbudowane porty: * 1x HDMI 1.4b
* 4x w tym min 3x USB 3.2, 1x USB4 z obsługą Thunderbolt 4
* port sieciowy RJ-45
* porty słuchawek i mikrofonu typu Combo
* czytnik kart pamięci

Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. |
| Klawiatura/mysz | * Klawiatura odporna na zalanie cieczą, układ US, klawiatura wyposażona w 2 stopniowe podświetlanie przycisków
* Mysz optyczna USB
 |
| Zasilacz | Energooszczędny zasilacz o mocy nie mniejszej niż 65W  |
| Bateria | Pozwalająca na nieprzerwaną pracę urządzenia do min. 6 godzin – do oferty należy załączyć test Mobile Mark 2018 lub kartę katalogową oferowanego komputera potwierdzającą czas pracy na zasilaniu bateryjnym. Ponadto komputer ma być wyposażony w system szybkiego ładowania akumulatora, który umożliwia szybkie naładowanie akumulatora notebooka w czasie 30 minut od 0% do 50%. |
| Bezpieczeństwo | * Moduł TPM 2.0
* Slot umożliwiający fizyczne zabezpieczenie komputera np. Kensington
* Wbudowany czytnik linii papilarnych w przycisku zasilania
 |
| System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
	1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
	2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych
2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego
3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim
4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.
5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe
6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim
9. Wbudowany system pomocy w języku polskim.
10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.
16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.
18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."
24. Wbudowany mechanizm wirtualizacji typu hypervisor."
25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.
26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób, aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.
30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.
31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM
33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.
34. Możliwość tworzenia wirtualnych kart inteligentnych.
35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)
36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.
37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
38. Mechanizmy logowania w oparciu o:
	1. Login i hasło,
	2. Karty inteligentne i certyfikaty (smartcard),
	3. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
	4. Certyfikat/Klucz i PIN
	5. Certyfikat/Klucz i uwierzytelnienie biometryczne
39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5
40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.
41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach
42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń
43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
 |
| BIOS  | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera.Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:* wersji BIOS
* nr seryjnym komputera
* Ilości zainstalowanej pamięci RAM
* typie procesora i jego prędkości
* informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS

 Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: * Możliwość ustawienia hasła Administratora
* Możliwość ustawienia hasła Użytkownika
* Możliwość ustawienia hasła dysku twardego
* Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS
* Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej.
* Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, karty WiFi, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, portów USB, bluetooth
 |
| Certyfikaty i standardy | * Certyfikat ISO9001 lub równoważny dla producenta sprzętu **(należy załączyć do oferty)**
* Deklaracja zgodności CE dla urządzenia **(należy załączyć do oferty)**
* Certyfikat lub inny dokument potwierdzający poprawną współpracę z zaoferowanym systemem operacyjnym **(należy załączyć do oferty)**
* Certyfikat ISO14001 lub równoważny dla producenta sprzętu (należy złożyć na etapie dostawy)
* Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki(należy złożyć na etapie dostawy)
 |
| Obudowa | Wykonana z metali lekkich lub kompozytów (np. aluminium, duraluminium, włókno węglowe, włókno szklane) charakteryzujących się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych.  |
| Waga urządzenia | Waga urządzenia z akumulatorem max. 1,50 kg |
| Bezpieczeństwo | * Złącze typu Kensington Lock
* Moduł TPM 2.0
 |
| Oprogramowanie | Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym, kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. Oprogramowanie musi zapewniać również ustawienie automatycznego uaktualnienia wszystkich sterowników we wskazanym dniu miesiąca. |
| Gwarancja | * 3 lata świadczona w miejscu użytkowania sprzętu (on-site)
* W przypadku awarii dysku twardego dysk uszkodzony pozostaje u Zamawiającego.
 |
| Wsparcie techniczne producenta | * możliwość weryfikacji u producenta konfiguracji fabrycznej i oferowanej zakupionego sprzętu
* możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji
* możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego
* naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub autoryzowanego partnera serwisowego producenta.
 |

**1.4. Oprogramowanie - pakiet zintegrowanych aplikacji biurowych – 30 kpl.**

1) Zamawiający wymaga dostarczenia licencji wieczystej oprogramowania w najnowszej na dzień składania ofert wersji, polskim interfejsie użytkownika, wyposażonego w następujące wbudowane funkcjonalności, bez użycia dodatkowych aplikacji:

* 1. dostępność pakietu w wersjach 32-bit oraz 64-bit, stały dostęp do najnowszych aktualizacji zakupionej wersji oprogramowania
	2. możliwość dostosowania dokumentów i szablonów do potrzeb użytkownika, oraz narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców

2) Wymagania odnośnie interfejsu użytkownika:

* 1. Pełna polska wersja językowa interfejsu użytkownika
	2. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych

3) Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:

* 1. posiada kompletny i publicznie dostępny opis formatu
	2. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526 ze zm.)
	3. umożliwia kreowanie plików w formacie XML
	4. wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES

4) W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).

5) Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.

6) Pakiet zintegrowanych aplikacji biurowych musi zawierać nieograniczone czasowo ani funkcjonalnie następujące składowe:

* 1. Edytor tekstów
	2. Arkusz kalkulacyjny
	3. Narzędzie do przygotowywania i prowadzenia prezentacji
	4. Narzędzie do zarządzania informacją prywatną

Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

7) Arkusz kalkulacyjny musi umożliwiać:

* 1. Tworzenie raportów tabelarycznych
	2. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
	3. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu
	4. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
	5. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
	6. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
	7. Wyszukiwanie i zamianę danych
	8. Wykonywanie analiz danych przy użyciu formatowania warunkowego
	9. Tworzenie wykresów prognoz i trendów na podstawie danych historycznych z użyciem algorytmu ETS
	10. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
	11. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
	12. Formatowanie czasu, daty i wartości finansowych z polskim formatem
	13. Zapis wielu arkuszy kalkulacyjnych w jednym pliku
	14. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł
	15. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po

najechaniu znacznikiem myszy na dany rodzaj wykresu)

* 1. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013, 2016, 2019, 365 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń
	2. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

8) Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

* 1. Przygotowywanie prezentacji multimedialnych, które będą:
* Prezentowanie przy użyciu projektora multimedialnego
* Drukowanie w formacie umożliwiającym robienie notatek
	1. Zapisanie jako prezentacja tylko do odczytu
	2. Nagrywanie narracji i dołączanie jej do prezentacji
	3. Opatrywanie slajdów notatkami dla prezentera
	4. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
	5. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
	6. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
	7. Możliwość tworzenia animacji obiektów i całych slajdów
	8. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu
	9. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013, 2016, 2019 i 365

9) Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:

1. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego
2. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych
3. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców
4. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną
5. Automatyczne grupowanie poczty o tym samym tytule
6. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy
7. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów
8. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie
9. Zarządzanie kalendarzem
10. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników
11. Przeglądanie kalendarza innych użytkowników
12. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach
13. Zarządzanie listą zadań
14. Zlecanie zadań innym użytkownikom
15. Zarządzanie listą kontaktów
16. Udostępnianie listy kontaktów innym użytkownikom
17. Przeglądanie listy kontaktów innych użytkowników
18. Możliwość przesyłania kontaktów innym użytkowników
19. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

**2. System do komunikacji on-line oraz wideokonferencji**

**2.1. Komputer MiniPC – 1 szt.**

|  |  |
| --- | --- |
| **Parametr lub** **warunek**  | **Minimalne wymagania**  |
| Procesor | Procesor klasy x86, zaprojektowany do pracy w komputerach mobilnych o wydajności nie mniejszej niż 10000 punktów na podstawie PerformanceTest w teście PASSMARK CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net na dzień składania ofert. Wynik oferowanego procesora w teście PASSMARK CPU Mark należy załączyć do oferty |
| Karta graficzna | Zintegrowana, liczba obsługiwanych wyświetlaczy: 4 |
| Pamięć operacyjna | 16GB, 3200MHz DDR4, 2 sloty na pamięć, z czego min. 1 wolny. Możliwość rozbudowy do 64GB pamięci RAM |
| Dysk twardy | SSD min. 256GB M.2 |
| Obudowa | Obudowa typu miniPC o sumie wymiarów nie przekraczających 28cm, obsługa dysków SATA M.2 i 2,5'', zasilacz zewnętrzny |
| Komunikacja | * LAN 10/100/1000
* WiFi 802.11 ax + Bluetooth
 |
| Czytnik kart pamięci | Tak |
| Porty/złącza | Wbudowane porty:* 1 x HDMI,
* 1 x mDP,
* 5 x USB w tym min.: 3x USB 3.1 Gen2 Typ-A, oraz 2x USB-C 3.1 Gen2 z obsługą Thunderbolt 3;
* port sieciowy RJ-45,
* porty słuchawek i mikrofonu
* czytnik kart pamięci

Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. |
| System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
	1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
	2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych
2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego
3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim
4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.
5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe
6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim
9. Wbudowany system pomocy w języku polskim.
10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.
16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.
18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."
24. Wbudowany mechanizm wirtualizacji typu hypervisor."
25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.
26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób, aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.
30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.
31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM
33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.
34. Możliwość tworzenia wirtualnych kart inteligentnych.
35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)
36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.
37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
38. Mechanizmy logowania w oparciu o:
	1. Login i hasło,
	2. Karty inteligentne i certyfikaty (smartcard),
	3. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
	4. Certyfikat/Klucz i PIN
	5. Certyfikat/Klucz i uwierzytelnienie biometryczne
39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5
40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.
41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach
42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń
43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
 |
| Certyfikaty i standardy | * Certyfikat ISO9001 lub równoważny dla producenta sprzętu **(należy załączyć do oferty)**
* Deklaracja zgodności CE dla urządzenia **(należy załączyć do oferty)**
* Certyfikat lub inny dokument potwierdzający poprawną współpracę z zaoferowanym systemem operacyjnym **(należy załączyć do oferty)**
* Certyfikat ISO14001 dla producenta sprzętu (należy złożyć na etapie dostawy )
 |
| Gwarancja | * 3 lata świadczona w miejscu użytkowania sprzętu (on-site)
* W przypadku awarii dysku twardego dysk uszkodzony pozostaje u Zamawiającego.
 |

**2.2. TV 49'' 4K Ultra HD – 1 szt.**

|  |  |
| --- | --- |
| **Parametr lub** **warunek**  | **Minimalne wymagania**  |
| Panel | LED |
| Przekątna ekranu | Min. 49" |
| Technologia HD | Ultra HD/4K |
| Rozdzielczość | 3840 x 2160 |
| Kontrast statyczny | Min. 5 000:1 |
| Tuner TV | * Analogowy
* DVB-S2
* DVB-T2/HEVC (H.265)
* DVB-C
 |
| Smart TV | Tak |
| System TV | * Smart TV
* WebOS
 |
| Obraz | * HDR10 Pro
* HLG
 |
| PVR/DVR | Tak |
| Max. moc głośników (sumaryczna) | 20 W |
| Tryb hotelowy | Tak |
| Bluetooth | Tak |
| WiFi | Tak |
| Gniazda we/wy | * 1 x 3,5 mm minijack
* 3 x HDMI
* 1 x USB 2.0
* 1 x RS-232 (COM)
* 1 x RJ-45 LAN
* 1 x Audio out
* 1 x Gniazdo CI/Cl+
 |
| Standard VESA | 200 x 200 |
| Pobór mocy | Max: 150W |
| Certyfikaty i standardy | * Certyfikat ISO9001 lub równoważny dla producenta sprzętu **(należy załączyć do oferty)**
* Deklaracja zgodności CE dla urządzenia **(należy załączyć do oferty )**
 |
| Gwarancja | 3 lata zgodnie z wymaganiami ogólnymi |

**2.3. Mobilny stojak do TV – 1 szt.**

|  |  |
| --- | --- |
| **Parametr lub** **warunek**  | **Minimalne wymagania**  |
| Przeznaczenie | Monitory/TV |
| Rodzaj | Statyw |
| Przekątna ekranu (min.) | 94 cm |
| Przekątna ekranu (maks.) | 178 cm |
| Standard VESA | 600 x 400 |
| Obciążenie (maks.) | 50 kg |
| Uchwyt narożny | Nie |
| Kolor | Czarny |
| Dodatkowe funkcje | kółka dla swobodnego przemieszczania |

**2.4. Zestaw głośnomówiący – 2 szt.**

|  |  |
| --- | --- |
| **Parametr lub**   **warunek**    | **Minimalne wymagania**    |
| Przeznaczenie  | Telefonia komórkowa  |
| Użytkowanie  | Średnia sala  |
| Komunikacja bezprzewodowa  | Bluetooth  |
| Złącza  | * 3,5 mm minijack
* 1 x USB 2.0
 |
| Dźwięk  | Stereo  |
| Kontrola dźwięku  | * Regulacja głośności
* Odbieranie/Wyciszanie połączenia
 |
| Funkcje bluetooth  | A2DP (Transmisja stereo)  |
| Mikrofon  | Tak  |
| Typ wbudowanego mikrofonu  | cyfrowe MEMS  |
| Dodatkowe wymagania  | * Plug and play
* Wyjątkowe mikrofony ZoomTalk
* Krystalicznie czysty dźwięk
 |
| Typ głośnika   | Pojedynczy głośnik  |
| Standardy łączności bezprzewodowej  | Min wersja. Bluetooth 4.1  |
| Wsparcie dla oprogramowania | Integracja i obsługa połączeń Microsoft Skype for Business, IBM Sametime, Cisco, Avayai Skype |
| Zasięg łączności bezprzewodowej  | Do 30m  |
| Czas rozmów  | Do 15h  |
| Redukcja szumów | Tak |
| Zasilanie | Akumulatorowe  |
| Długość przewodu połączeniowego  | Min. 1,2 m (przewód 3.5mm jack), 2,1 m (przewód USB)  |
| Zakres częstotliwości głośnika  | 100 Hz - 20 kHz  |
| Czułość głośnika  | 80dB  |
| Pasmo przenoszenia głośnika  | 100 Hz - 20 kHz  |
| Gwarancja | 3 lata zgodnie z wymaganiami ogólnymi |

**2.5. Kamera 4K – 2 szt.**

|  |  |
| --- | --- |
| **Parametr lub** **warunek**  | **Minimalne wymagania**  |
| PTZ | Tak |
| Typ produktu | Osobisty system wideokonferencji |
| System formatu sygnału analogowego | NTSC, PAL |
| Wsparcie dla montażu na tripodzie | Tak |
| Obsługiwane tryby wideo | 720p,1080p,2160p |
| Typ HD | 4K Ultra HD |
| Format obrazu | 16:9 |
| Wbudowane głośniki | Tak |
| Zasięg częstotliwości | 100 - 20000 Hz |
| Wbudowane głośniki | Tak |
| Liczba portów USB 2.0 | 2 |
| Gniazdko wyjścia DC | Tak |
| Obsługiwany typ USB | USB Type-A, USB Type-C |
| Liczba portów USB 2.0 | 2 |
| Gniazdko wyjścia DC | Tak |
| Cyfrowe zbliżenie | 4 x |
| Kąt pola widzenia (FOV) | 90 ° |
| Cyfrowe zbliżenie | 4 x |
| Częstotliwość mikrofonu | 50 - 14000 Hz |
| Liczba mikrofonów | 3 |
| Przewody | AC, USB Type-C |
| Gwarancja  | 3 lata zgodnie z wymaganiami ogólnymi |

**III. WARUNKI URUCHOMIENIA I ODBIORU WDROŻONYCH ROZWIĄZAŃ ORAZ**

**PRZEKAZANIA DO EKSPLOATACJI**

**1. Pozostałe wymagania od Wykonawców**

Poza dostawami i usługami podstawowymi, wykonawca jest zobowiązany do skalkulowania wszelkich usług pomocniczych, jakie uzna za niezbędne do prawidłowego wykonania przedmiotu zamówienia.

Wykonawca musi ponadto uwzględnić w cenie w ramach kosztów dodatkowych –

* koszty dostawy sprzętu na miejsce instalacji,
* koszty związane z zorganizowaniem pracy w sposób minimalizujący zakłócenie prowadzenia bieżącej działalności Zamawiającego,
* koszty testów, prób, badań, odbiorów technicznych – jeśli będą wymagane.

**2.  Dokumenty odbioru końcowego**

* Protokoły odbiorów częściowych.
* Protokoły z pomiarów i testów – jeśli dotyczy.
* Odpowiednie atesty i certyfikaty - jeśli są wymagane.
* Instrukcje obsługi, dokumentacje i inne dokumenty dostarczane wraz ze sprzętem, przez producenta.

**Część II**

**I. OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA I WYMAGAŃ ZAMAWIAJĄCEGO**

**1. Zakres przedmiotu zamówienia**

Przedmiotem zamówienia jest dostawa elementów, rozbudowa i modernizacja platform serwerowych oraz modernizacja i rekonfiguracja systemu archiwizacji i składowania danych, mająca na celu podniesienie poziomu bezpieczeństwa danych.

Wdrożenie tych systemów i rozwiązań ma również na celu podniesienie poziomu cyfryzacji Jednostki w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego **„Cyfrowa Gmina”** o numerze POPC.05.01.00-00-0001/21-00

**Szczegółowy zakres projektu składa się z następujących zadań:**

1. Rozbudowa i modernizacja platform serwerowych wraz z oprogramowaniem systemowym
* Serwer wirtualizacyjny - 1 kpl.
* Karta sieciowa 10G (do posiadanych serwerów) – 5 szt. i moduły SFP+ - 16 szt.
* Oprogramowanie systemowe do nowego serwera wirtualizacji – 1 lic.
* Oprogramowanie systemowe (doposażenie posiadanego serwera) – 1 lic.
* Licencje dostępowe dla użytkowników – 400 lic.
* Usługi instalacji, konfiguracji oraz wdrożenia – zgodnie z wcześniej opracowaną przez Wykonawcę koncepcją techniczną.
1. Rozbudowa i modernizacja systemu składowania i archiwizacji danych oraz wykonywania kopii zapasowych posiadanej macierzy dyskowej
* Dysk SSD, 1,92TB, SAS, 2,5 cala, ISSD (doposażenie posiadanej macierzy dyskowej) – 4 szt.
* Karta iSCSI 2x 10 Gbps (doposażenie posiadanej macierzy dyskowej) – 2 szt.
* Usługi instalacji, konfiguracji oraz wdrożenia – zgodnie z wcześniej opracowaną przez Wykonawcę koncepcją techniczną.

**2. Ogólne wymagania Zamawiającego**

Zamawiający dopuszcza rozwiązania równoważne w przypadku wskazania w opisie przedmiotu zamówienia norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy PZP.

- W przypadku podania przez Zamawiającego nazw materiałów, producentów czy znaków towarowych należy je traktować jako przykładowe, mające na celu doprecyzowanie przedmiotu zamówienia oraz określające standard techniczny i jakościowy. Zamawiający, wskazując oznaczenie konkretnego producenta lub konkretny produkt przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty i rozwiązania równoważne o nie gorszych parametrach jakościowych, technicznych, eksploatacyjnych i użytkowych. Ciężar wykazania spełnienia tych wymagań leży po stronie wykonawcy w składanej ofercie lub jeżeli ten przypadek ma miejsce w trakcie realizacji umowy – w chwili zaistnienia konieczności dokonania takiej zmiany.

- W przypadku zastosowania zasad wskazanych powyżej w trakcie realizacji umowy, mogą one wystąpić pod warunkiem, że zmiany te nie będą wpływać na oferowany w ofercie przedmiot zamówienia i efekt zakreślony niniejszym OPZ.

- W przypadku zastosowania materiałów, urządzeń, wyrobów lub rozwiązań równoważnych, Wykonawca zobowiązany jest do ich wskazania w ofercie oraz do złożenia wraz z ofertą kart technicznych lub innych dokumentów potwierdzających, że oferowane rozwiązania równoważne spełniają wymagania Zamawiającego opisane w przedmiocie zamówienia.

 **Wymagania ogólne dotyczące sprzętu:**

1) Wszystkie dostarczone urządzenia muszą być fabrycznie nowe, bez wad i uszkodzeń, nieregenerowane, nieużywane i nie będące przedmiotem wystaw i prezentacji oraz o ile nie wyspecyfikowano inaczej w wymaganiach szczegółowych dla urządzeń, wyprodukowane nie wcześniej niż 2021 roku.

2) Wszystkie urządzenia będą pochodziły z oficjalnego, europejskiego kanału dystrybucji.

3) Urządzenia zostaną dostarczone przez Wykonawcę własnym transportem i na własny koszt w miejsce wskazane przez Zamawiającego. Wszystkie urządzenia muszą być dostarczone w oryginalnych opakowaniach producenta.

4) Wszystkie urządzenia powinny być zgodne z normami UE i przeznaczone na rynek UE, oraz powinny posiadać certyfikat CE.

5) Dostarczany sprzęt powinien być kompletny i gotowy do uruchomienia, tak aby nie był konieczny zakup dodatkowych elementów czy akcesoriów.

6) Wykonawca dostarczy stosowne potwierdzenie gwarancji sprzętu i oprogramowania zapewniające, że sprzęt objęty jest gwarancją producenta.

7) Serwis sprzętu będzie świadczony przez producenta lub jego autoryzowanego partnera serwisowego posiadającego wdrożoną normę min. PN-EN ISO 9001 lub równoważną.

8) Sprzęt dostarczany w ramach niniejszego zamówienia, powinien być objęty 3 letnią gwarancją i wsparciem producenta, chyba że okres i warunki gwarancji zostały dodatkowo określony w opisie szczegółowym specyfikowanego wyposażenia/sprzętu. W okresie gwarancji Wykonawca jest zobowiązany zapewnić Zamawiającemu:

* 1. usuwanie wszelkich wad i nieprawidłowości powstałych na wskutek standardowej i zgodnej z przeznaczeniem eksploatacji przedmiotu zamówienia;
	2. przyjmowanie zgłoszeń serwisowych w godzinach 8.00-20.00 (faks lub e-mail) z możliwością zgłaszania awarii bezpośrednio u producenta (na wypadek braku reakcji serwisowej ze strony Wykonawcy);
	3. dostęp do bezpośredniego wsparcia technicznego producenta wraz z prawem do aktualizacji oprogramowania systemowego.

9) W ramach gwarancji wymagane jest wsparcie producenta sprzętu, a czas reakcji na zgłoszenia będzie realizowany w trybie następny dzień roboczy w miejscu instalacji i zastrzeżeniem, że uszkodzone nośniki danych pozostają u Zamawiającego. Ponadto wymagane jest, aby dostarczony poziom wsparcia producenta dawał możliwość kategoryzacji zgłoszeń i w przypadku awarii krytycznych gwarantował natychmiastową pomoc telefoniczną, szybką interwencję specjalisty ds. eskalacji zgłoszeń oraz wizytę serwisanta i/lub wysyłkę uszkodzonych części.

10) Udzielona gwarancja producenta nie wyłącza uprawnień Zamawiającego z tytułu rękojmi w stosunku do Wykonawcy.

**Wymagania ogólne dotyczące oprogramowania:**

Wykonawca zobowiązany jest dostarczyć Zamawiającemu:

1) certyfikaty licencyjne wystawione przez producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na dedykowanym portalu klienckim;

2) nośniki instalacyjne Oprogramowania, o ile nie są dostępne w formie elektronicznej na dedykowanym portalu klienckim;

3) adresy poczty elektronicznej, numery telefonów oraz inne dane dostępowe umożliwiające Zamawiającemu korzystanie ze Wsparcia technicznego świadczonego przez producenta Oprogramowania w pełnym zakresie, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;

4) zestawienie dostarczonych Zamawiającemu pozycji w zakresie Oprogramowania, zawierające m.in.: numer partii (SKU), pełna nazwa produktu, wersja i edycja oprogramowania, metryka licencyjna, rodzaj licencji (terminowa/bezterminowa), okres obowiązywania licencji, okres obowiązywania wsparcia technicznego, poziom wsparcia technicznego;

5) standardowe warunki licencyjne producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;

6) standardowe warunki Wsparcia technicznego producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;

7) oświadczenie producenta Oprogramowania potwierdzające dostawę licencji i objęcie ich wsparciem technicznym na poziomie zgodnym z wymaganiami Zamawiającego, o ile nie potwierdzają jej certyfikaty licencyjne i standardowe warunki Wsparcia technicznego.

Realizacja powyższego zakresu zamówienia musi być wykonana w oparciu o obowiązujące przepisy, przez Wykonawcę posiadającego stosowne doświadczenie, uprawnienia i potencjał wykonawczy oraz osoby o odpowiednich kwalifikacjach i doświadczeniu zawodowym.

**II. SZCZEGÓŁOWE WŁAŚCIWOŚCI I WYMAGANIA FUNKCJONALNO – UŻYTKOWE**

**1. Rozbudowa i modernizacja platform serwerowych wraz z oprogramowaniem systemowym**

**1.2. Koncepcja wdrożenia**

W ramach realizacji projektu dostarczony będzie serwer wirtualizacji, który wraz z jednym z istniejących serwerów, zostanie podłączony do nowego klastra niezawodnościowego. Pozostałe cztery z istniejących serwerów zostaną doposażone w 10cio gigabitowe dwuportowe karty sieciowe i nadal będą one pracowały poza klastrem w oparciu o już posiadane oprogramowanie MS Windows Server 2016. Dodatkowe karty 10G mają posłużyć do skomunikowania serwerów z rozbudowaną o dyski SSD macierzą SAN.

**1.3. Serwer wirtualizacyjny - 1 kpl.**

|  |  |
| --- | --- |
| Obudowa | * Typu RACK, wysokość nie więcej niż 2U;
* Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
* Ramię porządkujące ułożeni kabli z tyłu serwera;
 |
| Płyta główna | * Dwuprocesorowa;
* Wyprodukowana i zaprojektowana przez producenta serwera
* Możliwość instalacji procesorów 28-rdzeniowych;
* Zainstalowany moduł TPM 2.0;
* 4 złącza PCI Express generacji 3 w tym:
	+ 3 fizyczne złącza o prędkości x16;
	+ 1 fizyczne złącze o prędkości x8;
	+ Możliwość rozbudowy o riser umożliwiający instalację kart full height;
* 24 gniazda pamięci RAM;
* Obsługa minimum 3TB pamięci RAM DDR4;
* Wsparcie dla technologii:
	+ Memory Scrubbing
	+ SDDC
	+ ECC
* Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci)
* Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug;
 |
| Procesory | * 2 Procesory klasy x86 zaprojektowane do pracy w serwerach, każdy posiadający 20-rdzeni i częstotliwość bazową min. 2.1GHz, o łącznej wydajności nie mniejszej niż 41000 punktów na podstawie PerformanceTest w teście PASSMARK CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net na dzień składania ofert. Wynik oferowanego procesora w teście PASSMARK CPU Mark należy załączyć do oferty
 |
| Pamięć RAM | * 512 GB pamięci RAM
* DDR4 Registered
 |
| Dyski twarde i napędy | * Minimum 8 wnęk dla dysków twardych Hotplug;
* Zainstalowane 2 dyski SSD 480GB Hot Plug DWPD>=3.5;
* Możliwość instalacji wewnętrznej nagrywarki Blu-Ray;
 |
| Kontrolery LAN | * Karta LAN nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 4x 1Gbit Base-T, możliwość wymiany zainstalowanych interfejsów na 2x 25Gbit bez konieczności instalacji kart w slotach PCIe;
* Dodatkowa karta LAN 2x 10Gbit SFP+;
 |
| Kontrolery I/O | * Zainstalowany kontroler SAS RAID obsługujący poziomy 0,1,10,5,50,6,60 posiadający 8GB pamięci cache (opcjonalnie możliwość zabezpieczenia za pomocą baterii lub kondensatora)
 |
| Porty | * Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
* 2 port USB 3.0 na panelu przednim;
* 1 port USB 3.0 wewnętrzny;
* 2 porty USB 3.0 dostępne z tyłu serwera;
* Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;
* Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera;
 |
| Zasilanie, chłodzenie | * Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy minimalnej 800W;
* Redundantne wentylatory hotplug;
 |
| Zarządzanie | * Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii
	+ informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
		- karty rozszerzeń zainstalowane w dowolnym slocie PCI Express
		- procesory CPU
		- pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM
		- wbudowany na płycie głównej nośnik pamięci M.2 SSD
		- status karty zrządzającej serwera
		- wentylatory
		- bateria podtrzymująca ustawienia BIOS płyty główne
		- zasilacze

Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:* Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający zarządzanie, zdalny restart serwera;
	+ Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
	+ Dostęp poprzez przeglądarkę Web, SSH;
	+ Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
	+ Zarządzanie alarmami (zdarzenia poprzez SNMP)
	+ Możliwość przejęcia konsoli tekstowej
	+ Możliwość zarządzania przez min. 2 administratorów jednocześnie
	+ Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)
	+ Obsługa serwerów proxy (autentykacja)
	+ Obsługa VLAN
	+ Możliwość konfiguracji parametru Max. Transmission Unit (MTU)
	+ Wsparcie dla protokołu SSDP
	+ Obsługa protokołów TLS 1.2, SSL v3
	+ Obsługa protokołu LDAP
	+ Integracja z HP SIM
	+ Synchronizacja czasu poprzez protokół NTP
	+ Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej
* Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
* Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;
* Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
* Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.
 |
| Wspierane OS | * Microsoft Windows Server 2022, 2019, 2016
* VMWare vSphere 6.7, 7.0
* Suse Linux Enterprise Server 15
* Red Hat Enterprise Linux 7.9, 8
* Hyper-V Server 2016, 2019
 |
| Gwarancja  | * 5 lat gwarancji producenta serwera w trybie on-site z gwarantowaną wizytą technika w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.
* Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
* Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych ( dane tego podmiotu należy przekazać na etapie dostawy );
* Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
* Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty);
 |
| Dokumentacja, inne | * Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy lub producenta;
* Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;
* Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila, na który można zgłaszać usterki;
* W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
* Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
* Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %;
 |
| Certyfikaty i standardy | * Certyfikat ISO9001 dla producenta sprzętu **(należy załączyć do oferty)**
* Deklaracja zgodności CE dla urządzenia **(należy załączyć do oferty )**
* Oferowany serwer musi  poprawnie pracować z systemami Microsoft Windows Server 2022 oraz Vmware vSphere wersja min. 7.0

**(certyfikaty lub inne dokumenty potwierdzające należy załączyć do oferty)*** Certyfikat ISO14001 dla producenta sprzętu (należy złożyć na etapie dostawy )
* Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (należy złożyć na etapie dostawy )
 |

**1.4. Karta sieciowa 10G (do posiadanych serwerów) – 5 szt. i moduły SFP+ - 16 szt.**

|  |  |
| --- | --- |
| Rozbudowa posiadanych serwerów Fujitsu o numerach seryjnych:YMBQ004658YM6B010857YM6B012060YMBQ004659EWAG011534 | **5** szt. dwuportowych kart ETH 10G SFP+. Ze względów kompatybilności wymagane jest dostarczenia kart (**3** szt. QL41132 oraz **2** szt. X710-DA2);**16** szt. modułów SFP+ Multi Mode Fiber 10GbE LC;Oferowane elementy, muszą być produktami producenta serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta minimum 1 rok, dodatkowo, w przypadku instalacji w urządzeniu, elementy muszą przejąć reżim SLA tego urządzenia. |

W ramach rozbudowy serwerów pkt.1.4. wykonawca musi dokonać instalacji oraz konfiguracji na wskazanych przez Zamawiającego urządzeniach dostarczonego wyposażenia.

**1.5. Oprogramowanie systemowe do nowego serwera wirtualizacji – 1 lic.**

Licencja wieczysta na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz umożliwiać zainstalowanie nielimitowanej ilości instancji wirtualnych tego serwerowego systemu operacyjnego dla 40 rdzeni procesora. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. 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.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
	1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
	2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
	3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
	4. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
	1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
	2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
	1. Login i hasło,
	2. Karty z certyfikatami (smartcard),
	3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
	1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
		* Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
		* Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
		* Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
		* Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
	3. Zdalna dystrybucja oprogramowania na stacje robocze,
	4. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
	5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
		* Dystrybucję certyfikatów poprzez http,
		* Konsolidację CA dla wielu lasów domeny,
		* Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
		* Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
	6. Szyfrowanie plików i folderów.
	7. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
	8. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
	9. Serwis udostępniania stron WWW.
	10. Wsparcie dla protokołu IP w wersji 6 (IPv6).
	11. Wsparcie dla algorytmów Suite B (RFC 4869).
	12. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.
	13. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
		* Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
		* Obsługi ramek typu jumbo frames dla maszyn wirtualnych,
		* Obsługi 4-KB sektorów dysków,
		* Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
		* Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,
		* Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode).
26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

**1.6. Oprogramowanie systemowe (doposażenie posiadanego serwera) – 1 lic.**

Licencja wieczysta - grupowa, musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie nielimitowanych instancji wirtualnych tego serwerowego systemu operacyjnego dla 40 rdzeni procesora.

Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta i pozwalała na legalne używanie na oferowanym serwerze**.**

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. 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.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
	1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
	2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
	3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
	4. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
	1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
	2. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
	1. Login i hasło,
	2. Karty z certyfikatami (smartcard),
	3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
	1. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	2. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
		* Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
		* Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
		* Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
		* Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
	3. Zdalna dystrybucja oprogramowania na stacje robocze.
	4. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
	5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
		* Dystrybucję certyfikatów poprzez http,
		* Konsolidację CA dla wielu lasów domeny,
		* Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
		* Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
	6. Szyfrowanie plików i folderów.
	7. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
	8. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
	9. Serwis udostępniania stron WWW.
	10. Wsparcie dla protokołu IP w wersji 6 (IPv6).
	11. Wsparcie dla algorytmów Suite B (RFC 4869).
	12. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.
	13. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
		* Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
		* Obsługi ramek typu jumbo frames dla maszyn wirtualnych,
		* Obsługi 4-KB sektorów dysków,
		* Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
		* Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,
		* Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode).
26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

 Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

**1.7. Licencje dostępowe dla użytkowników – 400 licencji.**

Licencja wieczysta uprawniająca do legalnego korzystania z zasobów serwera przez min.400 użytkowników. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oprogramowania systemowego określonego w pkt. 1.5. i 1.6.

**2. Rozbudowa i modernizacja systemu składowania i archiwizacji danych oraz wykonywania kopii zapasowych posiadanej macierzy dyskowej**

**2.1. Koncepcja wdrożenia**

Aby w pełni wykorzystać moc obliczeniową węzłów klastra należy zapewnić odpowiednią wydajność po stronie dysków w macierzy oraz wysoką prędkość transmisji danych, należy wykonać rozbudowę istniejącej macierzy dyskowej SANo dodatkowe cztery dyski SSD o pojemności 1.92TB każdy oraz montaż dodatkowych kart sieciowych o prędkości do 10Gb/s.

W zakresie usług wdrożenia należy dodatkowo zainicjować wolumen z nowych dysków SSD, skonfigurować poziom redundancji oraz przygotować LUNy dla hostów wirtualizacji.

**2.2. Dysk SSD, 1,92TB, SAS, 2,5 cala, ISSD (doposażenie posiadanej macierzy dyskowej) –**

**4 szt. i Karta iSCSI 2x 10 Gbps (doposażenie posiadanej macierzy dyskowej) – 2 szt.**

|  |  |
| --- | --- |
| Rozbudowa posiadanej macierzy Fujitsu o numerze seryjnym4601647468 | 4 szt. dysków SSD 1,92 TB 2,5”2 dodatkowe interfejsy iSCSI 10G SFP+ do każdego z kontrolerów Oferowane elementy, muszą być produktami producenta macierzy lub być przez niego autoryzowane za zgodność ( tj. poprawną pracę ) oraz muszą być objęte gwarancją producenta minimum 1 rok, dodatkowo, w przypadku instalacji w urządzeniu, elementy muszą przejąć reżim SLA tego urządzenia. |

W ramach rozbudowy macierzy pkt. 2.2. wykonawca musi dokonać pełnej instalacji oraz konfiguracji na wskazanym przez Zamawiającego urządzeniu dostarczonego wyposażenia .

**III. WARUNKI URUCHOMIENIA I ODBIORU WDROŻONYCH ROZWIĄZAŃ ORAZ**  **PRZEKAZANIA DO EKSPLOATACJI**

**1. Pozostałe wymagania od Wykonawców**

Poza dostawami i usługami podstawowymi, wykonawca jest zobowiązany do skalkulowania wszelkich usług pomocniczych, jakie uzna za niezbędne do prawidłowego wykonania przedmiotu zamówienia dla przyjętej technologii, uwzględniając warunki ich wykonania.

Wykonawca musi ponadto uwzględnić w cenie w ramach kosztów dodatkowych:

* koszty dostawy sprzętu na miejsce instalacji,
* koszty związane z zorganizowaniem pracy w sposób minimalizujący zakłócenie prowadzenia bieżącej działalności Zamawiającego,
* koszty testów, prób, badań, odbiorów technicznych – jeśli będą wymagane.

**Uwaga!**

Podmioty realizujące zadania publiczne zobowiązane są do stosowania rozwiązań z zakresu interoperacyjności mi. na poziomie technologicznym. Interoperacyjność osiąga się poprzez stosowania minimalnych wymagań dla systemów teleinformatycznych. Zgodnie z §20 ust. 2 pkt. 12 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega mi. na:

* zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa,
* redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
* zapewnienia bezpieczeństwa plików,
* dbałość o aktualizację oprogramowania.

Dodatkowym ważnym elementem systemu jest możliwość rejestrowania i przechowywania zapisów w dziennikach systemowych (logowanie zdarzeń).

Konieczność zapewnienia tej funkcjonalności wynika z:

1. §21 ust. 1 KRI (zapewnienie rozliczalności w systemach teleinformatycznych w postaci elektronicznej),
2. Art. 22 i 23 Ustawy z dnia 5 lipca 2018 o Krajowym Systemie Cyberbezpieczeństwa

Wdrożone rozwiązania powinny spełniać wymagania przywołanych aktów prawnych oraz standardów rynkowych.

**2. Dokumenty odbioru końcowego**

* Protokoły odbiorów częściowych.
* Protokoły z pomiarów i testów – jeśli dotyczy.
* Odpowiednie atesty i certyfikaty - jeśli są wymagane.
* Instrukcje obsługi, dokumentacje i inne dokumenty dostarczane wraz ze sprzętem, przez producenta.

 **Część III**

**I. OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA I WYMAGAŃ ZAMAWIAJĄCEGO**

**1. Zakres przedmiotu zamówienia**

Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja urządzeń aktywnych sieci oraz systemu bezpieczeństwa. Ponadto zadaniem Wykonawcy będzie opracowanie koncepcji oraz wykonanie usług integratorskich. Zadania objęte zamówieniem mają na celu podniesienie poziomu cyfryzacji Jednostki w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego **„Cyfrowa Gmina”** o numerze POPC.05.01.00-00-0001/21-00

**Szczegółowy zakres projektu składa się z następujących zadań:**

1. Rozbudowa i modernizacja sieci LAN, doposażenie serwerowni
* Rozbudowa okablowania sieci LAN - 1 kpl.
* Przełącznik 10G (core: 48xSFP+, 4x100G) - wraz z pakietem gwarancyjno-serwisowym) – 2 szt.
* Przełącznik 48x GE RJ45, 4x 10GE SFP+ wraz z pakietem gwarancyjno-serwisowym – 3 szt.
* Przełącznik 24x GE RJ45, 4x 10GE SFP+ wraz z pakietem gwarancyjno-serwisowym – 1 szt.
* Usługi instalacji, konfiguracji oraz wdrożenia .

 2. System zapewnienia bezpieczeństwa teleinformatycznego (cyberbezpieczeństwo)

* + - UTM min. 18 x GE RJ45 – 1 kpl.
		- UTM Security, system logowania, raportowania i korelacji - 1 lic.

**2. Ogólne wymagania Zamawiającego**

Zamawiający dopuszcza rozwiązania równoważne w przypadku wskazania w opisie przedmiotu zamówienia norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy Pzp.

- W przypadku podania przez Zamawiającego nazw materiałów, producentów czy znaków towarowych należy je traktować jako przykładowe, mające na celu doprecyzowanie przedmiotu zamówienia oraz określające standard techniczny i jakościowy. Zamawiający, wskazując oznaczenie konkretnego producenta lub konkretny produkt przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty i rozwiązania równoważne o nie gorszych parametrach jakościowych, technicznych, eksploatacyjnych i użytkowych. Ciężar wykazania spełnienia tych wymagań leży po stronie wykonawcy w składanej ofercie lub jeżeli ten przypadek ma miejsce w trakcie realizacji umowy – w chwili zaistnienia konieczności dokonania takiej zmiany.

- W przypadku zastosowania zasad wskazanych powyżej w trakcie realizacji umowy, mogą one wystąpić pod warunkiem, że zmiany te nie będą wpływać na oferowany w ofercie przedmiot zamówienia i efekt zakreślony niniejszym OPZ.

- W przypadku zastosowania materiałów, urządzeń, wyrobów lub rozwiązań równoważnych, Wykonawca zobowiązany jest do ich wskazania w ofercie oraz do złożenia wraz z ofertą kart technicznych lub innych dokumentów potwierdzających, że oferowane rozwiązania równoważne spełniają wymagania Zamawiającego opisane w przedmiocie zamówienia.

**Wymagania ogólne dotyczące sprzętu:**

1) Wszystkie dostarczone urządzenia muszą być fabrycznie nowe, bez wad i uszkodzeń, nieregenerowane, nieużywane i nie będące przedmiotem wystaw i prezentacji oraz o ile nie wyspecyfikowano inaczej w wymaganiach szczegółowych dla urządzeń, wyprodukowane nie wcześniej niż 2021 roku.

2) Wszystkie urządzenia będą pochodziły z oficjalnego, europejskiego kanału dystrybucji.

3) Urządzenia zostaną dostarczone przez Wykonawcę własnym transportem i na własny koszt w miejsce wskazane przez Zamawiającego. Wszystkie urządzenia muszą być dostarczone w oryginalnych opakowaniach producenta.

4) Wszystkie urządzenia powinny być zgodne z normami UE i przeznaczone na rynek UE, oraz powinny posiadać certyfikat CE.

5) Dostarczany sprzęt powinien być kompletny i gotowy do uruchomienia, tak aby nie był konieczny zakup dodatkowych elementów czy akcesoriów.

6) Wykonawca dostarczy stosowne potwierdzenie gwarancji sprzętu i oprogramowania zapewniające, że sprzęt objęty jest gwarancją producenta.

7) Sprzęt dostarczany w ramach niniejszego zamówienia, powinien być objęty 12 miesięczną gwarancją i wsparciem producenta, chyba że okres i warunki gwarancji zostały dodatkowo określony w opisie szczegółowym specyfikowanego wyposażenia/sprzętu. W okresie gwarancji Wykonawca jest zobowiązany zapewnić Zamawiającemu:

a. usuwanie wszelkich wad i nieprawidłowości powstałych na wskutek standardowej i zgodnej z przeznaczeniem eksploatacji przedmiotu zamówienia,

b. przyjmowanie zgłoszeń serwisowych w godzinach 8.00-20.00 (faks lub e-mail) z możliwością zgłaszania awarii bezpośrednio u producenta (na wypadek braku reakcji serwisowej ze strony Wykonawcy),

c. dostęp do bezpośredniego wsparcia technicznego producenta wraz z prawem do aktualizacji oprogramowania systemowego.

8) Udzielona gwarancja producenta nie wyłącza uprawnień Zamawiającego z tytułu rękojmi w stosunku do Wykonawcy.

**Wymagania ogólne dotyczące oprogramowania:**

Wykonawca zobowiązany jest dostarczyć Zamawiającemu:

1) certyfikaty licencyjne wystawione przez producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na dedykowanym portalu klienckim;

2) nośniki instalacyjne Oprogramowania, o ile nie są dostępne w formie elektronicznej na dedykowanym portalu klienckim;

3) adresy poczty elektronicznej, numery telefonów oraz inne dane dostępowe umożliwiające Zamawiającemu korzystanie ze Wsparcia technicznego świadczonego przez producenta Oprogramowania w pełnym zakresie, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;

4) zestawienie dostarczonych Zamawiającemu pozycji w zakresie Oprogramowania, zawierające m.in.: numer partii (SKU), pełna nazwa produktu, wersja i edycja oprogramowania, metryka licencyjna, rodzaj licencji (terminowa/bezterminowa), okres obowiązywania licencji, okres obowiązywania wsparcia technicznego, poziom wsparcia technicznego;

5) standardowe warunki licencyjne producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;

6) standardowe warunki Wsparcia technicznego producenta Oprogramowania, o ile nie są dostępne w formie elektronicznej na ogólnodostępnym lub dedykowanym portalu klienckim;

Realizacja powyższego zakresu zamówienia musi być wykonana w oparciu o obowiązujące przepisy, przez Wykonawcę posiadającego stosowne doświadczenie, uprawnienia i potencjał wykonawczy oraz osoby o odpowiednich kwalifikacjach i doświadczeniu zawodowym.

**II. SZCZEGÓŁOWE WŁAŚCIWOŚCI I WYMAGANIA FUNKCJONALNO – UŻYTKOWE**

**1. Rozbudowa i modernizacja sieci LAN, doposażenie serwerowni**

**1.1. Rozbudowa okablowania sieci LAN – 1 kpl.**

**1.1.1. Koncepcja wdrożenia oraz rozbudowa i modernizacja sieci LAN**

Przed przystąpieniem do prac instalacyjno-montażowych, należy opracować koncepcję techniczną z szczegółowym opisem planowanych prac wraz z określeniem ryzyka związanego z działaniami podczas wykonywanych działań w zakresie rozbudowy i modernizacji sieci LAN oraz systemu bezpieczeństwa.

Koncepcja powinna obejmować:

1. część pasywną związaną z uporządkowaniem torów kablowych w szafach, poprawę organizacji kabli krosowych, uporządkowania urządzeń w szafach itp.
2. Część aktywną związaną z zaplanowaniem architektury sieci i zakresu konfiguracji urządzeń aktywnych oraz polityki bezpieczeństwa teleinformatycznego. Należy przygotować koncepcję wdrożenia uwzględniając hierarchiczny model projektowania i budowy sieci tj. wydzielając warstwę dystrybucyjną oraz dostępową.

Koncepcja techniczna powinna zostać przedstawiona i zatwierdzona przez Zamawiającego przed rozpoczęciem prac.

Na podstawie wcześniej opracowanej koncepcji technicznej, zatwierdzonej przez Zamawiającego, należy wykonać prace instalacyjno-montażowe oraz wdrożeniowe polegające na:

1. dostawie niezbędnych akcesoriów do montażu urządzeń i ich połączenia:
	* patchcordy światłowodów,
	* kable krosowe,
	* GigaBit Interface Converter,
	* organizatory kabli do szafy RACK.
2. uporządkowaniu okablowania w szafach serwerowych:
	* połączenia między przełącznikami,
	* połączenia przełączników z serwerami i urządzeniem UTM,
	* uporządkowanie i organizacja kabli krosowych w szafach.
3. fizycznym montażu urządzeń w lokalizacjach wyznaczonych przez Zamawiającego, instalacja będzie obejmować:
	* przełączniki CORE,
	* przełącznik DYSTRYBUCYJNE,
	* urządzenie UTM.
4. wykonaniu konfiguracji urządzeń aktywnych sieci LAN z uwzględnieniem hierarchicznego modelu projektowania i budowy sieci tj. wydzielając warstwę dystrybucyjną (przełączniki dystrybucyjny) oraz warstwę dostępową sieci (przełączniki dostępowe).

Zakres prac instalacyjno-wdrożeniowych powinien obejmować co najmniej:

* + aktualizację urządzenia do najnowszej i stabilnej wersji oraz rejestrację licencji, ponadto każdy przełącznik zostanie skonfigurowany w tryb centralnego zarządzania, oprócz ustawień systemowych, zostanie skonfigurowany interfejs sieciowy w celu komunikacji, który będzie obejmował statyczny adres IP i trasę routingu,
	+ przełączniki będą zarządzane z centralnej konsoli urządzenia UTM w tym celu Wykonawca zobowiązany jest do poprawnej komunikacji, autoryzacji urządzeń w konsoli urządzenia nadrzędnego,
	+ wykonanie segmentacji sieci w oparciu o technologię 802.1Q. (VLAN),
	+ Wdrożenie technologii do przechowywania logów, analizy i raportowania będzie obejmowała import systemu na wyznaczoną wirtualizację wraz z konfiguracją strefy czasowej z serwerem NTP, ponadto system powinien być zarejestrowany i posiadać aktywną licencję subskrypcyjną, oprócz ustawień wstępnych wykonawca jest zobowiązany do konfiguracji interfejsów, adresacji i routingu sieciowego,
	+ konfigurację mechanizmów STP,
	+ dodatkowo w celu ograniczenia niepożądanego ruchu w warstwie 2 wskazana jest izolacja poszczególnych komputerów (port isolation),
	+ agregacja portów na potrzeby połączeń z serwerami,
	+ Konfigurację ustawień systemowych:

- aktualizacja urządzenia,

- rejestracja urządzenia u producenta,

- aktywację licencji,

- konfiguracja strefy czasowej wraz z serwerem NTP,

- konfiguracja kont administracyjnych.

* + Konfigurację sieci:
	+ Konfigurację profili bezpieczeństwa:

- konfiguracja profilu IPS,

- konfiguracja profilu AntiVirus,

- konfiguracja profilu WebFilter,

- konfiguracja profilu DNS Filter,

- konfiguracja profilu Application Control,

- konfiguracja inspekcji SSL/SSH,

* + Konfigurację VPN

- IPSec Site-to-Site,

- IPSec Client-to-Site,

- konfiguracja SSL-VPN lub PPTP VPN,

- kont dla użytkowników SSL-VPN.

1. Konfiguracja urządzeń odpowiedzialnych za rozbudowę obecnej infrastruktury sieciowej
	* Konfiguracje ustawień systemowych:

- aktualizacja urządzenia,

- rejestrację urządzenia,

- aktywację licencji,

- konfiguracja strefy czasowej wraz z serwerem NTP,

- konfiguracje urządzenia w tryb zarządzany,

- konfiguracja kont administracyjnych,

* + Konfiguracja sieciowa:

- konfigurację portów SFP+,

- konfiguracja adresu IP,

- zbudowanie łączy agregacyjnych w oparciu o technologie LACP,

- konfiguracja vlan-ów na przełączniku,

1. Wdrożenie technologii w wersji subskrypcyjnej do analizy logów i raportowania, konfiguracja będzie obejmowała:
	* Konfiguracje ustawień systemowych:

- import maszyny na wyznaczoną wirtualizacją,

- konfiguracja strefy czasowej wraz z serwerem NTP,

- rejestrację urządzenia,

- aktywację licencji subskrypcyjnej.

* + Konfiguracja ustawień sieciowych:

- konfiguracja interfejsów,

- konfiguracja adresacji IPv4,

- konfiguracja routing,

- konfiguracja kont administracyjnych,

- proces autoryzacji i poprawnej komunikacji z urządzeniem brzegowym UTM.

1. Wykonawca przeprowadzi instruktaż dla administratora Zamawiającego w zakresie w/w zagadnień, w stopniu umożliwiającym administratorowi samodzielną konfigurację i administrację urządzeniami.

**1.2. Przełącznik 10G (core: 48xSFP+, 4x100G) - wraz z pakietem gwarancyjno-serwisowym – 2 szt.**

|  |  |
| --- | --- |
| **Parametr lub warunek**  | **Minimalne wymagania**  |
| Parametry fizyczne platformy  | * Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
* Zasilanie AC 230V.
* Wymagany - z możliwością wymiany w czasie pracy - redundantny zasilacz.
* Maksymalny pobór mocy: 185 W.
* Minimalny zakres temperatury pracy: 0-40ᵒC.
 |
| Interfejsy sieciowe  | Wymaganym jest, aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: * 48 porty 10 GE SFP+.
* 6 portów 40 GE QSFP+.
* 4 porty 100 GE QSFP28.
 |
| Zarządzanie  | * Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania.
* Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
* Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
* Wsparcie dla SNMP w wersjach 1-3
* Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
* Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
* Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
* Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
* Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
* Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
* Automatycznie wykonywane rewizje konfiguracji.
 |
| Parametry wydajnościowe   | * Przepustowość urządzenia - min. 1750 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 1518 Mpps.
* Tablica adresów MAC o pojemności co najmniej 144 k wpisów.
* Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund (<800ns)
 |
| Wymagane funkcje   | * Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
* Obsługa Jumbo Frames.
* Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
* Agregacja portów zgodna ze standardem 802.3ad.
* Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
* Obsługa routingu statycznego.
* Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP.
* Port-mirroring.
* Uwierzytelnianie 802.1x na poziomie portu.
* Uwierzytelnianie 802.1x w oparciu o adres MAC.
* W ramach 802.1x wsparcie dla dedykowanego VLANu dla gości (guest VLAN).
* W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
* W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
* Obsługa protokołu sFlow.
 |
| Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa  | 1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
* Centralne zarządzanie konfiguracją urządzenia.
* Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania.
* Centralne zarządzanie sieciami VLAN.
* Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u.
* Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.
* Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
* Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
* Automatyczna detekcja i rekomendacje konfiguracji.
* Przesyłanie logów na zewnętrzny serwer syslog.
* Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
* Obsługa białych i czarnych list adresów MAC.
* Wykrywanie aplikacji komunikujących się w sieci.
1. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
2. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

  |
| Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa  | 1. System musi realizować funkcję Stateful  Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
2. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
 |
| Gwarancja oraz wsparcie | System musi być objęty serwisem gwarancyjnym producenta przez okres 1 roku, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| Certyfikaty i standardy | * Certyfikat ISO9001 dla producenta sprzętu **(należy załączyć do oferty)**
* Deklaracja zgodności CE dla urządzenia **(należy załączyć do oferty )**
* Certyfikat ISO14001 dla producenta sprzętu (należy złożyć na etapie dostawy )
* Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (należy złożyć na etapie dostawy )
 |

**1.3. Przełącznik 48x GE RJ45, 4x 10GE SFP+ wraz z pakietem gwarancyjno-serwisowym – 3 szt.**

|  |  |
| --- | --- |
| **Parametr lub warunek**  | **Minimalne wymagania**  |
| Parametry fizyczne platformy  | * Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
* Zasilanie AC 230V.
* Maksymalny pobór mocy: 57 W.
* Minimalny zakres temperatury pracy: 0-45ᵒC.
 |
| Interfejsy sieciowe  | Wymaganym jest, aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: * 48 porty GE RJ-45.
* 4 porty 10 GE SFP+.
 |
| Zarządzanie  | * Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
* Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
* Wsparcie dla SNMP w wersjach 1-3
* Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
* Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
* Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
* Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
* Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
* Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
* Automatycznie wykonywane rewizje konfiguracji.
 |
| Parametry wydajnościowe   | * Przepustowość urządzenia - min. 176 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 260 Mpps.
* Tablica adresów MAC o pojemności co najmniej 32k wpisów.
* Opóźnienie wprowadzane przez przełącznik - poniżej 1 mikrosekund.
 |
| Wymagane funkcje   | * Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
* Obsługa Jumbo Frames.
* Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
* Agregacja portów zgodna ze standardem 802.3ad.
* Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
* Obsługa routingu statycznego.
* Port-mirroring.
* Uwierzytelnianie 802.1x na poziomie portu.
* Uwierzytelnianie 802.1x w oparciu o adres MAC.
* W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
* W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
* W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
* Obsługa protokołu sFlow.
 |
| Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa  | 1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
* Centralne zarządzanie konfiguracją urządzenia
* Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
* Centralne zarządzanie sieciami VLAN.
* Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
* Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.
* Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
* Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
* Automatyczna detekcja i rekomendacje konfiguracji.
* Przesyłanie logów na zewnętrzny serwer syslog.
* Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
* Obsługa białych i czarnych list adresów MAC.
* Wykrywanie aplikacji komunikujących się w sieci.
* Musi być możliwe redundantne połączenie z elementami zarządzającymi.
* W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
* Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
* Obsługa białych i czarnych list adresów MAC.
* Wykrywanie aplikacji komunikujących się w sieci.
1. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
2. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

  |
| Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa  | 1. System musi realizować funkcję Stateful  Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
2. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
 |
| Gwarancja oraz wsparcie  | System musi być objęty serwisem gwarancyjnym producenta przez okres 1 roku, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.   |
| Certyfikaty i standardy | * Certyfikat ISO9001 dla producenta sprzętu **(należy załączyć do oferty)**
* Deklaracja zgodności CE dla urządzenia **(należy załączyć do oferty)**
* Certyfikat ISO14001 dla producenta sprzętu (należy złożyć na etapie dostawy )
* Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (należy złożyć na etapie dostawy )
 |

**1.4. Przełącznik 24x GE RJ45, 4x 10GE SFP+ wraz z pakietem gwarancyjno-serwisowym – 1 szt.**

|  |  |
| --- | --- |
| **Parametr lub warunek**  | **Minimalne wymagania**  |
| Parametry fizyczne platformy  | * Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
* Zasilanie AC 230V.
* Maksymalny pobór mocy: 26,3 W.
* Minimalny zakres temperatury pracy: 0-45ᵒC.
 |
| Interfejsy sieciowe  | Wymaganym jest, aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: * 24 porty GE RJ-45.
* 4 porty 10 GE SFP+.
 |
| Zarządzanie  | * Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
* Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
* Wsparcie dla SNMP w wersjach 1-3
* Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
* Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
* Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
* Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
* Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
* Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
* Automatycznie wykonywane rewizje konfiguracji.

  |
| Parametry wydajnościowe   | * Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps.
* Tablica adresów MAC o pojemności co najmniej 32k wpisów.
* Opóźnienie wprowadzane przez przełącznik - poniżej 1 mikrosekund.
 |
| Wymagane funkcje   | * Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
* Obsługa Jumbo Frames.
* Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
* Agregacja portów zgodna ze standardem 802.3ad.
* Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
* Obsługa routingu statycznego.
* Port-mirroring.
* Uwierzytelnianie 802.1x na poziomie portu.
* Uwierzytelnianie 802.1x w oparciu o adres MAC.
* W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
* W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
* W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
* Obsługa protokołu sFlow.
 |
| Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa  | 1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
* Centralne zarządzanie konfiguracją urządzenia
* Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
* Centralne zarządzanie sieciami VLAN.
* Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
* Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.
* Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
* Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
* Automatyczna detekcja i rekomendacje konfiguracji.
* Przesyłanie logów na zewnętrzny serwer syslog.
* Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
* Obsługa białych i czarnych list adresów MAC.
* Wykrywanie aplikacji komunikujących się w sieci.
* Musi być możliwe redundantne połączenie z elementami zarządzającymi.
* W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.
* Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
* Obsługa białych i czarnych list adresów MAC.
* Wykrywanie aplikacji komunikujących się w sieci.
1. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
2. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

  |
| Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa  | 1. System musi realizować funkcję Stateful  Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
2. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
 |
| Gwarancja oraz wsparcie  | System musi być objęty serwisem gwarancyjnym producenta przez okres 1 roku, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.    |
| Certyfikaty i standardy | * Certyfikat ISO9001 dla producenta sprzętu **(należy załączyć do oferty)**
* Deklaracja zgodności CE dla urządzenia **(należy załączyć do oferty )**
* Certyfikat ISO14001 dla producenta sprzętu (należy złożyć na etapie dostawy )
* Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (należy złożyć na etapie

dostawy ) |

**2. System zapewnienia bezpieczeństwa teleinformatycznego (cyberbezpieczeństwo**)

**2.1. UTM min. 18 x GE RJ45 – 1 kpl.**

|  |  |
| --- | --- |
| **Parametr lub warunek**  | **Minimalne wymagania**  |
| Wymagania Ogólne   | 1. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
2. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
3. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
4. System musi wspierać IPv4 oraz IPv6 w zakresie:
* Firewall
* Ochrony w warstwie aplikacji
* Protokołów routingu dynamicznego
 |
| Redundancja, monitoring i wykrywanie awarii    | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
 |
| Interfejsy, Dysk, Zasilanie  | 1. System realizujący funkcję Firewall musi dysponować minimum:
* 18 portami Gigabit Ethernet RJ-45.
* 8 gniazdami SFP 1 Gbps.
* 4 gniazdami SFP+ 10 Gbps.
1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 4000 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System musi być wyposażony w zasilanie AC.
 |
| Parametry wydajnościowe  | 1. W zakresie Firewall’a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz 280 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 27 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 13 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 13 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 3 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4 Gbps.
 |
| Funkcje Systemu Bezpieczeństwa   | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: * Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
* Kontrola Aplikacji.
* Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
* Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
* Ochrona przed atakami - Intrusion Prevention System.
* Kontrola stron WWW.
* Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
* Zarządzanie pasmem (QoS, Traffic shaping).
* Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
* 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.
* Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
* Analiza ruchu szyfrowanego protokołem SSH.
* Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

  |
| Polityki, Firewall   | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (ApplicationLevel Gateway) dla protokołu SIP.
1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash’e złośliwych plików.
3. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu:
* Amazon Web Services (AWS).
* Microsoft Azure
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.

  |
|  Połączenia VPN   | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
* Wsparcie dla IKE v1 oraz v2.
* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman  grup 19 i 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.
1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

  |
| Routing i obsługa łączy WAN   | W zakresie routingu rozwiązanie powinno zapewniać obsługę: * Routingu statycznego.
* Policy Based Routingu.
* Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
 |
| Funkcje SD-WAN   | 1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
 |
| Zarządzanie pasmem   | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

  |
| Ochrona przed malware   | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. 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.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
 |
| Ochrona przed atakami   | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

  |
| Kontrola aplikacji  | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
 |
| Kontrola WWW  | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
 |
| Uwierzytelnianie użytkowników w ramach sesji  | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
 |
| Zarządzanie  | 1. 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.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
 |
| Logowanie   | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. 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.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.
 |
| Certyfikaty  | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: * ICSA lub EAL4 dla funkcji Firewall **(należy załączyć do oferty)**
* Certyfikat ISO9001 dla producenta sprzętu **(należy załączyć do oferty)**
* Deklaracja zgodności CE dla urządzenia **(należy załączyć do oferty )**
* Certyfikat ISO14001 dla producenta sprzętu (należy złożyć na etapie dostawy )
* Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (należy złożyć na etapie dostawy )
 |
| Gwarancja, wsparcie | 1. System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 1 roku.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący powinien posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7 Wymagania powinny być potwierdzone dokumentami:
* Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej) – oświadczenie należy załączyć na etapie dostawy .
 |
| Serwisy i licencje | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:* Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 1 roku.
* Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzęń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Sygnatury ochrony systemów przemysłowych SCADA na okres 1 roku.
 |

**2.2. UTM Security, system logowania, raportowania i korelacji - 1 lic.**

|  |  |
| --- | --- |
| **Parametr lub warunek**  | **Minimalne wymagania**  |
| Wymagania ogólne | 1. W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.
2. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi wersje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).
 |
| Interfejsy, Dysk | System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 5 TB. |
| Parametry wydajnościowe | 1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów. |
| W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje: |
| Logowanie | 1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
* Listę najczęściej wykrywanych ataków.
* Listę najbardziej aktywnych użytkowników.
* Listę najczęściej wykorzystywanych aplikacji.
* Listę najczęściej odwiedzanych stron www.
* Listę krajów, do których nawiązywane są połączenia.
* Listę najczęściej wykorzystywanych polityk Firewall.
* Informacje o realizowanych połączeniach IPSec.
1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
2. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
3. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
 |
| Raportowanie | W zakresie raportowania system musi zapewniać:* Generowanie raportów co najmniej w formatach: PDF, CSV.
* Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
* Funkcję definiowania własnych raportów.
* Możliwość spolszczenia raportów.
* Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.
 |
| Korelacja logów | W zakresie korelacji zdarzeń system musi zapewniać:1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
* Malware.
* Aplikacje sieciowe.
* Email.
* IPS.
* Traffic.
* Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
1. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.
 |
| Zarządzanie | 1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. * Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi. |
| Serwisy i licencje | Wsparcie: System musi być objęty serwisem producenta przez okres 1 roku, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. |

**III. WARUNKI URUCHOMIENIA I ODBIORU WDROŻONYCH ROZWIĄZAŃ ORAZ PRZEKAZANIA DO EKSPLOATACJI**

**1. Pozostałe wymagania od Wykonawców**

Poza dostawami i usługami podstawowymi, wykonawca jest zobowiązany do skalkulowania wszelkich usług pomocniczych, jakie uzna za niezbędne do prawidłowego wykonania przedmiotu zamówienia dla przyjętej technologii, uwzględniając warunki ich wykonania.

Wykonawca musi ponadto uwzględnić w cenie w ramach kosztów dodatkowych –

* koszty dostawy sprzętu na miejsce instalacji,
* koszty zabezpieczenia istniejących elementów obiektuoraz wyposażenia (urządzeń) Użytkownika przed ich zniszczeniem w trakcie wykonywania prac,
* koszty związane z zorganizowaniem pracy w sposób minimalizujący zakłócenie prowadzenia bieżącej działalności Zamawiającego,
* koszty zapewnienia bezpieczeństwa bhp i ppoż. w trakcie realizacji prac,
* koszty testów, prób, badań, odbiorów technicznych – jeśli będą wymagane,
* koszty opracowania dokumentacji powykonawczej,
* koszty przeprowadzenia instruktażu dla administratora Zamawiającego w zakresie zagadnień objętych zamówieniem w stopniu umożliwiającym administratorowi samodzielną konfigurację i administrację urządzeniami.

**Uwaga!**

Podmioty realizujące zadania publiczne zobowiązane są do stosowania rozwiązań z zakresu interoperacyjności mi. na poziomie technologicznym. Interoperacyjność osiąga się poprzez stosowania minimalnych wymagań dla systemów teleinformatycznych. Zgodnie z §20 ust. 2 pkt. 12 Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (KRI) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega mi. na:

- zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa,

- redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

- zapewnienia bezpieczeństwa plików,

- dbałość o aktualizację oprogramowania,

Dodatkowym ważnym elementem systemu jest możliwość rejestrowania i przechowywania zapisów w dziennikach systemowych (logowanie zdarzeń).

Konieczność zapewnienia tej funkcjonalności wynika z:

1. §21 ust. 1 KRI (zapewnienie rozliczalności w systemach teleinformatycznych w postaci elektronicznej),
2. Art. 22 i 23 Ustawy z dnia 5 lipca 2018 o Krajowym Systemie Cyberbezpieczeństwa

Wdrożone rozwiązania powinny spełniać wymagania przywołanych aktów prawnych oraz standardów rynkowych.

**2. Dokumenty odbioru końcowego**

* Protokoły odbiorów częściowych
* Protokoły z pomiarów i testów – jeśli dotyczy
* Odpowiednie atesty i certyfikaty - jeśli są wymagane
* Instrukcje obsługi, dokumentacje i inne dokumenty dostarczane wraz ze sprzętem, przez producenta
* Dokumentacja powykonawcza.