Załącznik nr 1a do SWZ – RG.271.11.2022

Szczegółowy opis przedmiotu zamówienia
Specyfikacja techniczna

DOSTAWA SPRZĘTU KOMPUTEROWEGO W RAMACH WDROŻENIA E-USŁUG DLA MIESZKAŃCÓW GMINY CHŁOPICE – CYFRYZACJA ORAZ PODNIESIENIE CYBERBEZPIECZEŃSTWA W SIECI LAN

Nazwa komponentu lub warunek	***Wymagane minimalne parametry techniczne***	***Oferowane parametry Spełnia TAK/NIE***
1. Komputer biurkowy – AiO - 10 sztuk		
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.	Producent: ……. Model: …….
Ekran	Przekątna: min 21,3" (+/- 0,3 cala) Rozdzielczość: min. FHD 1080p (1920x1080), podświetlenie LED, 250nits, format 16:9, kontrast 1000:1, kąty widzenia 178°, matryca matowa wykonana w technologii WVA/MVA/IPS/PLS	Spełnia TAK/NIE
Obudowa	- musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) - zintegrowana z monitorem (AIO) - podstawa musi umożliwiać regulację kąta nachylenia w zakresie co najmniej –5° do przodu oraz 29° do tyłu, wysokości w zakresie 70 – 80 mm - obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem seryjnym, PN pozwalającym na jednoznaczna identyfikacje zaoferowanej konfiguracji	Spełnia TAK/NIE
Chipset	Dostosowany do zaoferowanego procesora	Spełnia TAK/NIE
Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera umożliwiająca konfigurację wielodyskową min. SATAIII + M.2 PCIe	Spełnia TAK/NIE

Procesor	Procesor klasy x86, minimum 6 rdzeniowy, zaprojektowany do pracy w komputerach przenośnych, taktowany zegarem o częstotliwości 2.7 GHz (maks. częstotliwość turbo 4,6 GHz), z pamięcią cache CPU co najmniej 12 MB lub równoważny procesor klasy x86 osiągający w teście Passmark CPU Mark wynik min.: 17628 punktów **(wynik zaproponowanego procesora musi znajdować się na stronie http://www.cpubenchmark.net) – wydruk ze strony należy dołączyć do oferty**.	Ilość punktów ……. Spełnia TAK/NIE
Pamięć operacyjna	Min. 8GB minimum 3200MHz z możliwością rozszerzenia do 64 GB	Ilość GB: …….. Spełnia TAK/NIE
Dysk twardy	Min. 256GB SSD M.2 PCIe NVMe oraz zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.	Ilość GB:…… Spełnia TAK/NIE
Napęd optyczny	Nagrywarka DVD +/-RW	Spełnia TAK/NIE
Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia pamięci.	Spełnia TAK/NIE
Audio/Video	Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo 2 x 2W, wbudowane dwa mikrofony, wbudowana kamera 1080p z wbudowaną mechaniczną przesłoną umożliwiającą fizyczne zasłonięcie kamery, kamera obsługująca Windows Hello	Spełnia TAK/NIE
Porty/złącza	Wbudowane (minimum): DisplayPort, 6 x USB3.2 (z czego jeden umożliwiający szybkie ładowanie urządzeń zewnętrznych/podłączanych nawet przy wyłączonym komputerze), czytnik kart multimedialnych, 1 x RJ 45 (LAN), 1 x wyjście na słuchawki i mikrofon (Combo), Wśród portów USB wymaga się, aby przynajmniej jeden port był w standardzie USB-C 3.2 Gen 2. Wymagana ilość portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.	Spełnia TAK/NIE

Klawiatura/mysz	Klawiatura przewodowa w układzie US. Mysz przewodowa z rolką (scroll)	Spełnia TAK/NIE
Karta sieciowa	Port sieci LAN 100/1000 Ethernet RJ 45 zintegrowany z płytą główną.	Spełnia TAK/NIE
Zasilacz	Energooszczędny zasilacz o mocy nie większej niż 150W oraz sprawności min. 89%.	Spełnia TAK/NIE
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. 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	Spełnia TAK/NIE

	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: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. 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	
System operacyjny	Licencja na system operacyjny Microsoft Windows 10 Home, zainstalowany system operacyjny Windows 10 Home niewymagający ręcznej aktywacji za pomocą telefonu lub Internetu w firmie Microsoft lub system równoważny. Opis równoważności zawiera Zał. 1 Opis równoważności	Spełnia TAK/NIE

BIOS	BIOS zgodny ze specyfikacją UEFI **Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o:** - modelu komputera, PN - numerze seryjnym, - Numer inwentarzowy, - MAC Adres karty sieciowej, - wersja i data BIOS - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM, - stanie pracy wentylatora - informacja o licencji na system operacyjny **Możliwość z poziomu Bios:** - wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy oraz z boku obudowy. - wyłączenia karty sieciowej (WIFI i LAN), karty audio, mikrofonu, kamery, czytnika kart multimedialnych - możliwość wyłączenia wirtualizacji w BIOS - możliwość zaprogramowania automatycznego włączenia komputera o określonej porze - możliwość ustawienia portów USB w jednym z dwóch trybów: 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 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 - możliwość ustawienia następujących haseł: hasła administratora, hasła Power-On, hasła na dysk twardy - dostęp do systemu logowania zdarzeń w BIOS. System musi zapewniać logowanie co najmniej takich zdarzeń jak: update BIOS, zmiany w konfiguracji, wyczyszczenie logów - obsługa Bios za pomocą klawiatury i myszy	Spełnia TAK/NIE

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 płyty głównej Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: PC: Producent, model 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 System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.	Spełnia TAK/NIE
Certyfikaty i standardy	Dla producenta sprzętu należy dostarczyć: Certyfikat ISO9001 dla producenta sprzętu Urządzenie musi spełniać: Deklarację zgodności ENERGY STAR	Spełnia TAK/NIE
Waga/rozmiary urządzenia	Waga urządzenia wraz ze stopą max. 9 kg	Spełnia TAK/NIE
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji.	Spełnia TAK/NIE
Bezpieczeństwo	Złącze typu Kensington Lock Moduł dTPM 2.0 Wbudowana mechaniczna zasłona kamery	Spełnia TAK/NIE

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.	Spełnia TAK/NIE
Gwarancja	min. 3 lata gwarancji producenta świadczona w miejscu użytkowania sprzętu (on-site) lub zgodnie z kryteriami oceny ofert	Spełnia TAK/NIE
Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego. - możliwość weryfikacji u producenta konfiguracji fabrycznej 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.	Spełnia TAK/NIE
2. Urządzenie wielofunkcyjne z funkcją skanowania – 1 szt.		
Typ urządzenia	urządzenie wielofunkcyjne: LASER MONO	Producent: …….. Model: ……
Prędkość druku	mono min. 29 stron A4 na minutę,	Spełnia TAK/NIE
Miesięczne obciążenie	do 20000 stron	Spełnia TAK/NIE
maksymalna pamięć	64 MB	Spełnia TAK/NIE
szybkość procesora	Min 500 MHz	Spełnia TAK/NIE

optyczna rozdzielczość skanowania	do 600x600 dpi	Spełnia TAK/NIE
kodowanie koloru	24 bit	Spełnia TAK/NIE
rozdzielczość kopiowania	do **600x600** dpi	Spełnia TAK/NIE
Porty komunikacyjne	Min 1x ethernet - druk w sieci LAN wireless - druk przez WiFi drukowanie z chmury z dedykowanej aplikacji producenta	Spełnia TAK/NIE
Parametry wydruku	automatyczny druk dwustronny automatyczny podajnik dokumentów (ADF) min 40 stron	Spełnia TAK/NIE
pojemność głównego podajnika papieru	Min 150 stron	Spełnia TAK/NIE
3. Urządzenie wielofunkcyjne z opcją skanowania – 1 szt.		
Typ urządzenia	urządzenie wielofunkcyjne: drukarka kolorowa, kopiarka kolorowa, skaner kolorowy	Producent: …… Model: ……
Prędkość druku	mono i kolor min. 24 stron A4 na minutę, min. 15 stron A3 na minutę	Spełnia TAK/NIE
Technologia druku	laserowa kolorowa C,M,Y,K	Spełnia TAK/NIE
Panel dotykowy / rozdzielczość	Panel dotykowy o minimalnej przekątnej 10,1" oraz rozdzielczości 1024 x 600 personalizowany w języku polskim, z możliwością wyświetlania interfejsów zewnętrznych aplikacji np. do zarządzania wydrukiem, systemów OCR.	Spełnia TAK/NIE
Maksymalny format papieru	nie mniejszy niż SRA3, możliwość wydruku banderowego	Spełnia TAK/NIE
Czas nagrzewania	nie więcej niż 14 sekundy	Spełnia TAK/NIE
Czas wykonania pierwszej kopii	nie więcej niż 5,2 sekund mono, nie więcej niż 6,9 sekundy kolor	Spełnia TAK/NIE

Wejściowa obsługa papieru	co najmniej 2 kasety uniwersalne o pojemności nie mniejszej niż 500 arkuszy każda, taca ręczna o pojemności nie mniejszej niż 150 arkuszy	Spełnia TAK/NIE
Obsługiwana gramatura papieru	co najmniej w zakresie od 52 do 300 g/m^2	Spełnia TAK/NIE
Automatyczny podajnik dokumentów	wymagany, z funkcją odwracania, o pojemności nie mniejszej niż 100 arkuszy, obsługujący formaty A6-A3; w gramaturze 35-128 g/m^2	Spełnia TAK/NIE
Prędkość skanowania	Min. 80 oryginałów/min. (300 dpi) zarówno w kolorze jak i w mono	Spełnia TAK/NIE
Funkcja zoom	co najmniej w zakresie od 25-400% w odstępach 0.1% ; automatyczne powiększenie	Spełnia TAK/NIE
Zużycie Energii	co najmniej w zakresie od 25-400% w odstępach 0.1% ; automatyczne powiększenie	Spełnia TAK/NIE
Kopiowanie wielokrotne	co najmniej w zakresie 1 - 9,999	Spełnia TAK/NIE
Zainstalowana pamięć	min. 7,0 GB RAM oraz twardy dysk SSD o pojemności min. 250 GB	Spełnia TAK/NIE
Język drukarki	PCL 6; PCL 5c; PostScript 3 (CPSI 3016); XPS	Spełnia TAK/NIE
Zawansowane funkcje drukowania	Aplikacja która umożliwia drukowanie z pozycji komputera bez instalacji sterownika za pomocą „przeciąg i puść". Umożliwiająca: - Tworzenie Hot folderów do bezpośredniego druku - Skojarzenie specyficznych ustawień z hot folderami - Automatyczne zapisywanie plików w folderach „druku" - Obsługuje PDF, TIFF, PCL i PS	Spełnia TAK/NIE
Protokoły sieciowe	TCP/IP (IPv4/IPv6); SMB; LPD; IPP; SNMP; HTTP(S); AppleTalk; Bonjour	Spełnia TAK/NIE
Rozdzielczość kopiowania i skanowania	nie mniejsza niż 600 x 600 dpi	Spełnia TAK/NIE
Rozdzielczość drukowania	Nie mniejsza niż 1,800 x 600 - 1,200 x 1,200	Spełnia TAK/NIE
Funkcje drukarki	bezpośredni druk PDF, bezpośredni druk z pamięci USB	Spełnia TAK/NIE

Tryby skanera	Kolorowy sieciowy z możliwością skanowania - Skanowania na adres e-mail (Scan-to-Me) - Skanowanie do SMB (Scan-to-Home) - Skanowanie do FTP - Skanowanie do skrzynki (HDD) - Skanowanie do USB - Skanowanie do WebDAV - Skanowanie do DPWS - Skanowanie sieciowe TWAIN	Spełnia TAK/NIE
Wyjściowe formaty plików skanera	JPEG; TIFF; PDF; PDF/A; kompaktowy PDF; szyfrowany PDF; przeszukiwany PDF ; XPS; kompaktowy XPS; PPTX; DOCX, XLSX, RTF,TXT	Spełnia TAK/NIE
Szafka pod urządzenie	Wymagana, metalowa na kółkach. Zamawiający wymaga szafki w kolorach odpowiadającym kolorom urządzenia	Spełnia TAK/NIE
Funkcje monitorująco raportujące	Aplikacja umożliwiająca po przez przeglądarkę internetową, dodawanie użytkowników (do 1000 kont użytkowników; obsługa również Active Directory (login + hasło + e-mail + katalog SMB)) z możliwością definiowania uprawnień do danych funkcji urządzenia np. Wydruku: mono / kolor, Kopia Mono / Kolor Skanowanie. Rozwiązanie winno umożliwiać również możliwość raportowania ilości wykonanych wydruków / kopii / skanów, poszczególnych użytkowników wpisanych do systemu. System musi posiadać autoryzacje użytkowania na maszynie za pomocą: Identyfikatora, login / hasło System winien umożliwiać funkcję wydruk wstrzymany i poufny.	Spełnia TAK/NIE
Wymagane oprogramowanie	Aplikacja umożliwiająca zgłaszanie przez użytkowników problemów z urządzeniem – możliwość zgłoszenia problemów z działaniem urządzenia bezpośrednio z panelu urządzenia na zdefiniowany wcześniej e-mail. W przypadku problemów z wydrukiem istnieje możliwość załączenia skanu dokumentu oraz wpisania komentarza bezpośrednio z panelu urządzenia. Aplikacja musi mieć możliwość zgłaszania następujących predefiniowanych problemów: Uszkodzenie mechaniczne, Problem z kasetą papieru, Problem z podajnikiem ADF, Głośna praca urządzenia, Zacinanie papieru, Nie pobiera papieru, Zła jakość wydruku, Zabrudzenia na wydruku, Pognieciony wydruk, Nie można odebrać wydruku, Wydruk niepoprawny	Spełnia TAK/NIE

Zawansowane funkcje bezpieczeństwa	- Zmiana Hasła Administratora (Indywidualne 16 znakowe hasło alfanumeryczne). - Szyfrowanie całej zawartości dysku twardego (Indywidualny 20-znakowy klucz szyfrujący). - Zabezpieczenie hasłem dysku twardego (Indywidualne 20-znakowe hasło alfanumeryczne). - Tymczasowe nadpisywanie danych w celu wyeliminowania wszelkich śladów danych (Klient może wybrać pomiędzy pojedynczym lub potrójnym nadpisywaniem). - Automatyczne usuwanie prac i związanych materiałów znajdujących się w elektronicznych folderach (Klient może wybrać żądane ustawienie czasu).	Spełnia TAK/NIE
Materiały eksploatacyjne	Toner czarny dostarczony z urządzeniem pozwalający na wydrukowanie minimum 28.000 stron A4 przy zadruku 5% oraz tonery cyan, magenta, yellow dostarczone z urządzeniem pozwalające na wydrukowanie minimum 28.000 stron A4 przy zadruku 5%,	Spełnia TAK/NIE
Wymagania gwarancji.	Urządzenie winno mieć wykupiony min 24 miesięcznym pakiet gwarancji producenta sprzętu. Urządzenie musi być fabrycznie nowe. Sprzęt musi pochodzić z autoryzowanego przez jej producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich.	Spełnia TAK/NIE
4. Jednostka Serwerowa KPL – 1 szt.		
Typ urządzenia	Jednostka serwerowa	Producent: ……. Model: ……
Obudowa	Typu RACK, wysokość nie więcej niż 2U; Szyny umożliwiające wysunięcie serwera z szafy stelażowej; Możliwość zainstalowania 10 dysków twardych hot plug 3,5"; Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych; Zainstalowany napęd DVD-RW; Możliwość zainstalowania dedykowanego wewnętrznego napędu	Spełnia TAK/NIE

Płyta główna	Dwuprocesorowa; Wyprodukowana i zaprojektowana przez producenta serwera Możliwość instalacji procesorów 38-rdzeniowych; Możliwość zainstalowania modułu TPM 2.0; 7 złącz PCI Express generacji 4 w tym: 4 fizyczne złącza o prędkości x16; 3 fizyczne złącza o prędkości x8; Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości; Opcjonalnie możliwość uzyskania 8 aktywnych złącz PCI-e; 32 gniazda pamięci RAM; Obsługa minimum 4TB pamięci RAM ; Obsługa minimum 12TB pamięci RAM DDR4 + pamięć nieulotna Wsparcie dla technologii: Memory Scrubbing SDDC ECC Memory Mirroring ADDDC; 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;	Spełnia TAK/NIE
Procesory	Zainstalowany co najmniej 1 procesor klasy x86_64 min 12 rdzeniowy, zaprojektowany do pracy w komputerach przenośnych, taktowany zegarem o częstotliwości 2.1 GHz lub równoważny procesor klasy x86 zapewniający wydajność min. 23580 pkt. (dla pojedynczego procesora) w teście Passmark CPU Mark, znajdujący się na liście https://www.cpubenchmark.net/cpu_list.php **Do oferty należy dołączyć wydruk ze strony.**	Ilość punktów ……. Spełnia TAK/NIE
Pamięć RAM	Min 64 GB pamięci o taktowaniu minimum 3200 Mhz	Ilość GB: …….. Spełnia TAK/NIE

Dyski twarde	Minimum 8 wnęk dla dysków twardych Hotplug Zainstalowane 6 dysków SSD SATA minimum 480GB HOT PLUG 3.5" Zainstalowane 2 dyski SATA minimum 2TB HOT PLUG	Spełnia TAK/NIE
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 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;	Spełnia TAK/NIE
Kontrolery I/O	Zainstalowany kontroler SAS RAID obsługujący poziomy 0,1,10,5,50,6,60 posiadający 2GB pamięci cache (opcjonalnie możliwość zabezpieczenia za pomocą baterii lub kondensatora)	Spełnia TAK/NIE
Porty	Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; 2 port USB 3.0 wewnętrzne; 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; 2 porty USB 3.0 na panelu przednim	Spełnia TAK/NIE
Zasilanie, chłodzenie	Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; 2 port USB 3.0 wewnętrzne; 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; 2 porty USB 3.0 na panelu przednim	Spełnia TAK/NIE
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	Spełnia TAK/NIE

	- 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 6 administratorów jednocześnie - Opcjonalne 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); - Opcjonalna dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB; - Opcjonalna 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 opcjonalnie 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. - BIOS UEFI w specyfikacji 2.7;	
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, 8.3 - Hyper-V Server 2016, 2019	Spełnia TAK/NIE
Gwarancja	min. 5 lat gwarancji producenta serwera w trybie onsite z gwarantowanym przyjazdem do miejsca użytkowania sprzętu certyfikowanego przez producenta pracownika serwisu do końca następnego dnia roboczego <u>lub zgodnie z kryteriami oceny ofert;</u> Zgłaszanie usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu (bez udziału administratora); Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; 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;	Spełnia TAK/NIE
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 **<u>– wymaganie oświadczenie wykonawcy;</u>** Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE –	Spełnia TAK/NIE

	wymagane oświadczenie wykonawcy; 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 %; Zgodność z normami: CB, RoHS, WEEE, GS oraz CE; Przedstawić certyfikat	strona producenta urządzenia ……
5. Licencja systemu serwerowego – 1 szt.		
Oprogramowanie	Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Wymaga się, aby oferowane licencje umożliwiały korzystanie 28 użytkownikom. 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.	Nazwa systemu: ……. Spełnia TAK/NIE

	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: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) 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: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) 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: a) Login i hasło, b) Karty z certyfikatami (smartcard), c) 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: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) 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: i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.	

	iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i. Dystrybucję certyfikatów poprzez http ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m) 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: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy	

	węzłami klastra v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. 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	
6. Urządzenie NAS wraz z dyskami – 1 szt.		
Urządzenie	Urządzenie do pracy w sieci	Producent: …… Model: ……
Model CPU	zaprojektowany do pracy w urządzeniach przenośnych , taktowany zegarem o częstotliwości min 2,0 GHz (maks. częstotliwość turbo 2,9 GHz), z pamięcią cache CPU co najmniej 4 MB lub równoważny procesor osiągający w teście Passmark CPU Mark wynik min.: 1713 punktów (wynik zaproponowanego procesora musi znajdować się na stronie http://www.cpubenchmark.net) – **wydruk ze strony należy dołączyć do oferty**	Ilość punktów …….. Spełnia TAK/NIE
Liczba procesorów	Min 1	Spełnia TAK/NIE
Architektura procesora	64-bit	Spełnia TAK/NIE

Pamięć systemowa	Min 2 GB	Ilość GB: ……. Spełnia TAK/NIE
Całkowita liczba gniazd pamięci	1	Spełnia TAK/NIE
Maksymalna pojemność pamięci	Min 6 GB	Ilość GB: ……. Spełnia TAK/NIE
Kieszeń/kieszenie na dyski	Min 4	Spełnia TAK/NIE
Kieszenie dysków M.2 2 (NVMe)	Min 2	Spełnia TAK/NIE
Zainstalowane dyski zgodne z tabelą kompatybilności producenta urządzenia	Min 4 x 6 TB Pamięć podręczna 256MB - Prędkość obrotowa 7200 obr./min - Niezawodność 1 000 000 godz.	Ilość GB: ……. Spełnia TAK/NIE
Zgodny typ dysków obsługiwanych	3.5" SATA HDD 2.5" SATA HDD 2.5" SATA SSD M.2 2280 NVMe SSD	Spełnia TAK/NIE
Port LAN RJ-45 1GbE z obsługą funkcji Link Aggregation / przełączania awaryjnego	Min 2 szt	Spełnia TAK/NIE
Port USB 3.2 1. generacji	Min 2 szt	Spełnia TAK/NIE
Gwarancja	Minimum 36 miesięcy	Spełnia TAK/NIE

7. Rozbudowa zabezpieczeń logicznych – Firewall - 1 szt		
Urządzenie	Urządzenie do pracy w sieci	Producent: …… Model: ……
Redundancja, monitoring i wykrywanie awarii	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. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.	Spełnia TAK/NIE
Interfejsy, Dysk, Zasilanie	System realizujący funkcję Firewall musi dysponować minimum: 5 portami Gigabit Ethernet RJ-45. System musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. W ramach systemu powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. System musi być wyposażony w zasilanie AC.	Spełnia TAK/NIE
Parametry wydajnościowe	W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. 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 1.4 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.	Spełnia TAK/NIE

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). • Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. • Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. • 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	Spełnia TAK/NIE
Polityki, Firewall	Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych	Spełnia TAK/NIE

	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	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. 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.	Spełnia TAK/NIE

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.	Spełnia TAK/NIE
Funkcje SD-WAN	System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.	Spełnia TAK/NIE
Zarządzanie pasmem	System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.	Spełnia TAK/NIE
Ochrona przed malware	Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 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. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.	Spełnia TAK/NIE
Ochrona przed atakami	Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	Spełnia TAK/NIE

	Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 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. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	
Kontrola aplikacji	Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	Spełnia TAK/NIE
Kontrola WWW	Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 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. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.	Spełnia TAK/NIE

Uwierzytelnianie użytkowników w ramach sesji	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. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.	Spełnia TAK/NIE
Zarządzanie	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. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.	Spełnia TAK/NIE
Logowanie	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. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie	Spełnia TAK/NIE

	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. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Musi istnieć możliwość logowania do serwera SYSLOG.	
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall.	Spełnia TAK/NIE
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: a) 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 36 miesięcy.	Spełnia TAK/NIE
Gwarancja oraz wsparcie	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, 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.	Spełnia TAK/NIE
Rozszerzone wsparcie serwisowe	System musi być 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 36 miesięcy.	Spełnia TAK/NIE

Załącznik nr 1 Opis równoważności systemu operacyjnego.

Windows 10 Home lub równoważny system operacyjny. System dostarczony razem z certyfikatem licencyjnym (certyfikat obejmujący wersję 64bit).Warunki równoważności systemu operacyjnego:
System, poprzez mechanizmy wbudowane, bez użycia dodatkowych aplikacji, musi:
1) umożliwiać instalację oprogramowania, wymienionego poniżej:
- Microsoft Office 2016/2019

2) umożliwiać dokonywanie aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
3) zapewniać internetową aktualizację w języku polskim;
4) posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
5) posiadać zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;
6) posiadać wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi);
7) posiadać wbudowany system pomocy w języku polskim;
8) dostarczać wsparcie dla .NET Framework 1.1, 2.0, 3.0 i 4.5 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;
9) posiadać graficzne środowisko instalacji i konfiguracji.
10) posiadać wbudowane następujące mechanizmy umożliwiające przystosowanie stanowiska dla osób niepełnosprawnych:
- lupa powiększająca zawartość ekranu,
- narrator odczytujący zawartość ekranu,
- regulacja jasności i kontrastu ekranu,
- możliwość odwrócenia kolorów np. biały tekst na czarnym tle,
- regulowanie rozmiaru kursora myszy i czasu trwania powiadomień systemowych,
- funkcja sterowania myszą z klawiatury numerycznej,
- funkcja klawiszy trwałych, która sprawia, że skrót klawiszowy jest uruchamiany po naciśnięciu jednego klawisza,
- funkcja napisów w treściach wideo,
- możliwość skorzystania z wizualnych rozwiązań alternatywnych wobec dźwięków".

Dostarczany sprzęt musi być fabrycznie nowy, musi posiadać niezbędne okablowanie, zasilacze oraz wszystkie inne komponenty, zapewniające właściwą instalację i użytkowanie (np. przewody zasilające itp).

Dla jednoznacznej identyfikacji oferowanego sprzętu należy podać co najmniej nazwę producenta, a także nazwę, model i konfigurację oferowanego sprzętu. Zamawiający wymaga również podania faktycznych parametrów sprzętu w taki sposób, by oceniający byli w stanie stwierdzić, czy zaoferowany sprzęt spełnia wymagania specyfikacji oraz dołączenie kart katalogowych oferowanych urządzeń dla potwierdzenia spełnienia wymaganych minimalnych parametrów technicznych.

(kwalifikowany podpis elektroniczny lub podpis zaufany lub podpis osobisty osoby upoważnionej do reprezentowania Wykonawcy)