

Załącznik nr 1 do OPZ PO ZMIANIE

Wymagane minimalne parametry techniczne

1. Komputer All-In-One dla Urzędu Miasta Zgierza – 55 szt.

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Typ	Komputer stacjonarny. Typu All in One, komputer fabrycznie wbudowany w obudowę monitora. W ofercie wymagane jest podanie modelu producenta komputera.
2.	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
3.	Wydajność obliczeniowa	Procesor wielordzeniowy osiągający w teście PassMark CPU Mark wynik min. 9900 punktów według wyników ze strony https://www.cpubenchmark.net
4.	Pamięć RAM	16GB DDR4 2666MHz możliwość rozbudowy do 64GB, jeden slot wolny
5.	Pamięć masowa	256GB SSD M.2 NVMe Możliwość instalacji dodatkowego dysku twardego
6.	Wydajność grafiki	Grafika zintegrowana z procesorem powinna umożliwiać pracę min. dwumonitorową, współdzielona i dynamicznie przydzielana pamięć z RAM
7.	Matryca	Rozmiar matrycy / plamki
		min.21.5" / max. 0,24mm
		Rozdzielczość
		FHD (1920x1080)
		Jasność typowa
		min. 250 cd/m ²
		Kontrast typowy
8.	Wyposażenie multimedialne	700:1
		Barwa koloru (typowa)
		72% NTSC
		Kąty widzenia
		178 (+/- 89)
9.	Obudowa	Rodzaj matrycy
		Matowa IPS
8.	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki min. 2W na kanał. Wbudowana w obudowę matrycy cyfrowa kamera 2,0 MP z diodą LED informującą użytkownika o pracy, Mechanicznie chowana w obudowie (nie dopuszcza się kamer przekręcanych i wystających poza obrys obudowy) Wbudowany w obudowę mikrofon
9.	Obudowa	Typu All-in-One zintegrowana z monitorem min. 21,5". Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki), Demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi. Komputer musi posiadać możliwość zainstalowania na ścianie przy wykorzystaniu ściennego systemu montażowego VESA 100, Zasilacz zewnętrzny o mocy max. 130W. Wbudowany w obudowie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System musi zapisywać logi zdarzeń w BIOS. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji. Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz wpisany na stałe w BIOS. Podstawa jednostki typu All – in – One musi umożliwiać: Regulację pochyłu pionowego w zakresie od -5 do 30 stopni. Regulację wysokości w zakresie minimum 10 cm. Ustawienie jednostki w trybie Pivot. Obrót podstawy w lewą oraz prawą stronę.
10.	Zgodność z systemami operacyjnymi	Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzającego certyfikację).

	i standardami	
11.	Bezpieczeństwo	<p>Płyta główna zawierająca układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego.</p> <p>Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot'owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, Internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego.</p> <p>Czujnik otwarcia obudowy, musi zbierać zdarzenia i zapisywać je w BIOS</p>
12.	Wirtualizacja	<p>Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu.</p>
13.	BIOS	<p>BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą myszy. (przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury).</p> <p>Informacje dostępne z poziomu BIOS na potrzeby inwentaryzacji: wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach, procesor (typ, nazwa, typowa prędkość, minimalna, maksymalna, cache L2 i L3) , pojemności zainstalowanego lub zainstalowanych dysków twardej MAC adres zintegrowanej karty sieciowej, zintegrowany układ graficzny, kontroler audio.</p> <p>Informacje dostępne w samym menu BIOS bez stosowania dodatkowego oprogramowania jak i wbudowanego systemu diagnostycznego.</p> <p>Możliwość, ustawienia hasła na poziomie: - administratora [hasło nadrzędne] - użytkownika/systemowego [hasło umożliwiające użytkownikowi zmianę swojego hasła i zgodnie z uprawnieniami nadanymi przez administratora dokonywać zmian ustawień BIOS], rozruch systemu operacyjnego [hasło blokuje start systemu operacyjnego]. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń. Możliwość wyłączenia/włączenia karty sieciowej Możliwość włączenia/wyłączenia kontrolera SATA Możliwość włączenia/wyłączenia kontrolera audio, Możliwość włączenia/wyłączenia układu TPM. Możliwość włączenia/wyłączenia wbudowanej kamery i czytnika kart multimedialnych Możliwość włączenia/wyłączenia czujnika otwarcia obudowy, ustawienia go w tryb cichy Możliwość przypisania w BIOS numeru nadawanego przez Administratora oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym. [musi umożliwiać znaki specjalne (@#\$\$%^)]. Możliwość zdefiniowania automatycznego uruchamiania komputera w min. dwóch trybach: codziennie lub w wybrane dni tygodnia, Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość wyłączania portów USB w szczególności pojedynczo w dowolnej kombinacja. BIOS musi nanosić automatycznie wszystkie zmiany konfiguracji dotyczące w szczególności: pamięci, procesora, dysku.</p>
14.	Certyfikaty i standardy	<p>Urządzenia muszą być wyprodukowane zgodnie z norą ISO 9001 oraz 50001 (certyfikaty załączyć do oferty).</p> <p>Deklaracja zgodności CE (załączyć do oferty).</p> <p>Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS</p>

		Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram Certyfikat TCO - do oferty załączyć certyfikat lub wydruk ze strony http://tcocertified.com/product-finder/
15.	Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy jałowej dysku twardego (IDLE) wynosząca maksymalnie 24 dB (załączyć oświadczenie producenta).
16.	System Operacyjny	Zainstalowany system operacyjny Windows 10 Professional zgodnie z wytycznymi z punktu 5.
17.	Wymagania dodatkowe	<p>Wbudowane porty:</p> <p>1x DP++ 1.4/HDCP 2.3 port</p> <p>1x USB 3.2 Gen 2 Type-C port</p> <p>3x USB 3.2 Gen 1 Type-A port</p> <p>2x USB 2.0</p> <p>Wymagane porty USB wbudowane, nie dopuszcza się stosowania rozgałęziaczy, hub'ów itp.</p> <p>1x Universal audio jack z boku lub dołu obudowy</p> <p>1x One Line-out audio</p> <p>1x RJ-45 port 10/100/1000 Mbps</p> <p>Czytnik kart SD min. 3.0</p> <p>Karta WiFi ac+ bluetooth 5</p> <p>Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, min. 1 złącze M.2 2280 dla dysku twardego oraz 1 złącze M.2 karty WiFi</p> <p>Klawiatura USB w układzie: polski programisty</p> <p>Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll)</p> <p>Wbudowany napęd DVD RW</p>
18.	Dodatkowe oprogramowanie	<p>Oprogramowanie producenta komputera z nieograniczoną czasowo licencją na użytkowanie umożliwiające:</p> <ul style="list-style-type: none"> - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi - dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji - sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania) - dostęp do wykazu wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku *.xml <p>Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku.</p>

		W ofercie należy podać nazwę oprogramowania
19.	Wsparcie techniczne	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego)
20.	Warunki gwarancji	Gwarancja 36 miesięcy, producenta, świadczona na miejscu u klienta. Czas reakcji serwisu - do końca następnego dnia roboczego. W przypadku awarii dysk twardy zostaje u Zamawiającego – oświadczenie podmiotu realizującego serwis lub producenta o spełnieniu tego warunku wymagane będzie przed podpisaniem umowy. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – oświadczenie Producenta potwierdzonego, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta wymagane będzie przed podpisaniem umowy. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem – wymagane będzie przed podpisaniem umowy.

2. Komputer przenośny (laptop) – 35 szt.

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Zastosowanie	Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
2.	Matryca	Matryca o przekątnej 15.6" z powłoką przeciwoodblaskową i rozdzielczością 1920 x 1080. Jasność matrycy 250 cd/m2, kontrast min. 700:1
3.	Procesor	Procesor osiągający w teście PassMark Performance Test, co najmniej 10000 punktów w kategorii Average CPU Mark. Wynik dostępny na stronie: https://www.cpubenchmark.net/cpu_list.php
4.	Pamięć RAM	8GB DDR4 3200MHz możliwość rozbudowy do min 32GB, min. jeden wolny slot pamięci na dalszą rozbudowę
5.	Pamięć masowa	Min. 256GB SSD NVMe Możliwość zainstalowania dodatkowego dysku 2,5"
6.	Karta graficzna	Zintegrowana z procesorem
7.	Klawiatura	Klawiatura w układzie US – QWERTY z wydzieloną klawiaturą numeryczną oraz z wbudowanym w klawiaturze podświetleniem. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12.
8.	Multimedia	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2 x 2W. Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy. Kamera internetowa z diodą informującą o aktywności, 0.9 Mpix, trwale zainstalowana w obudowie matrycy wyposażona w mechaniczną przysłonę. Czytnik kart multimedialnych w formacie microSD. Złącze audio typu combo (słuchawki i mikrofon).
9.	Łączność bezprzewodowa	Karta Wireless AX 2x2 + Bluetooth 5.1
10.	Bateria i zasilanie	Min. 54Whr umożliwiającą jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin.

		Zasilacz o mocy min. 65W.
11.	Waga	Waga max 2 kg z baterią.
12.	Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane, uszczelnienie dookoła matrycy chroniące klawiaturę notebooka, po zamknięciu przed kurzem i wilgocią. Kąt otwarcia notebooka min 180 stopni. Komputer spełniający normy MIL-STD-810H (załączyć oświadczenie producenta).
13.	BIOS	BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego (wmontowanego na stałe). Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: dacie produkcji komputera (data produkcji nieusuwalna), o kontrolerze audio, procesorze, a w szczególności min. i maks osiąganą prędkości, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne (nieedytowalne) pole asset tag, nie podlegające skasowaniu nawet po aktualizacji BIOS. Funkcja logowania się do BIOS na podstawie hasła użytkownika i administratora (hasła niezależne), możliwość ustawienia haseł administratora oraz użytkownika składających się z małych liter, dużych liter, cyfr, znaków specjalnych. BIOS zawierający informację o stanie naładowania baterii, mocy podpiętego zasilacza, ponadto możliwość zarządzania trybem ładowania baterii (np. określenie docelowego poziomu naładowania). Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS. Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym.
14.	Certyfikaty	Certyfikat ISO9001 dla producenta sprzętu (należy załączyć do oferty). Certyfikat ISO 50001 dla producenta sprzętu (należy załączyć do oferty). Deklaracja zgodności CE (załączyć do oferty). Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki. Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony). EnergyStar – załączyć do oferty certyfikat lub wydruk ze strony. Certyfikat EPEAT min. Silver dla Polski.
15.	Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 22dB (załączyć oświadczenie producenta).
16.	Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych i dodatkowych nośników pamięci masowej oraz dostępu do Internetu i sieci lokalnej.
17.	Bezpieczeństwo	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej. Czytnik linii papilarnych.
18.	System operacyjny	Zainstalowany system operacyjny Windows 10 Professional zgodnie z wytycznymi z punktu 5.

19.	Oprogramowanie dodatkowe	<p>Zainstalowane oprogramowanie z bezterminową licencją do wykonywania aktualizacji systemu i jego zasobów umożliwiające:</p> <ul style="list-style-type: none"> - określenie preferencji aktualizacji; - ustawienie priorytetu aktualizacji; - użycia opcji planowania aktualizacji bieżących wersji sterowników. <p>Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające:</p> <ol style="list-style-type: none"> 1) upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji; 2) możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji: <ul style="list-style-type: none"> a) o poprawkach i usprawnieniach dotyczących aktualizacji; b) dacie wydania ostatniej aktualizacji; c) priorytecie aktualizacji; d) zgodność z systemami operacyjnymi; e) jakiego komponentu sprzętu dotyczy aktualizacja; f) wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e. 3) wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne; 4) możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga; 5) rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr); 6) sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania); 7) dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml; 8) raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
20.	Porty i złącza	Wbudowane porty i złącza: 1 x HDMI 1.4, 1x RJ-45, 1 x USB 2.0, 2 x USB 3.2 typu A, w tym jeden dosilony, 1x USB 3.2 gen 2 typu C, port zasilania, 1 x RJ-45, gniazdo linki zabezpieczającej.
21.	Wsparcie techniczne	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego)
22.	Warunki gwarancyjne	Gwarancja 36 miesięcy, producenta, świadczona na miejscu u klienta. Czas reakcji serwisu – do końca następnego dnia roboczego.

		<p>Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzację producenta komputera – dokumenty potwierdzające załączyć do oferty.</p> <p>Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem wymagane będzie przed podpisaniem umowy.</p> <p>W przypadku awarii dysk twardy zostaje u Zamawiającego – oświadczenie podmiotu realizującego serwis lub producenta o spełnieniu tego warunku wymagane będzie przed podpisaniem umowy.</p> <p>Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.</p> <p>Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).</p>
--	--	--

3. Router WiFi z modemem GSM LTE – 35 szt.

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Typ	Router mobilny WiFi z modemem GSM LTE
2.	Architektura sieci	FastEthernet
3.	Porty wbudowane	3 x 10/100 Mbit/s 1 x WAN (RJ-45) 1 x Slot karty SIM
4.	Obsługiwane standardy sieci GSM	4G: FDD-LTE B1/B3/B7/B8/B20 (2100/1800/2600/900/800 MHz) TDD-LTE B38/B40/B41 (2600/2300/2500 MHz) 3G: DC-HSPA+/HSPA+/HSPA/UMTS B1/B8 (2100/900 MHz)
5.	Obsługiwane standardy WiFi	802.11a 802.11b 802.11g 802.11n 802.11ac
6.	Pasmo	2,4 GHz 5 GHz
7.	Ilość anten	2 wewnętrzne anteny LTE 2 zintegrowane anteny Wi-fi
8.	Bezpieczeństwo	64/128-bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK
9.	Warunki gwarancji	36 miesięcy w trybie: Door to door.

4. Komputer All-In-One dla jednostek oświatowych – 50 szt.

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Typ	Komputer stacjonarny. Typu All in One, komputer fabrycznie wbudowany w obudowę monitora. W ofercie wymagane jest podanie modelu producenta komputera.
2.	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
3.	Wydajność obliczeniowa	Procesor wielordzeniowy osiągający w teście PassMark CPU Mark wynik min. 9900 punktów według wyników ze strony https://www.cpubenchmark.net
4.	Pamięć RAM	8GB DDR4 2666MHz możliwość rozbudowy do 64GB, jeden slot wolny.

5.	Pamięć masowa	256GB SSD M.2 NVMe. Możliwość instalacji dodatkowego dysku twardego.	
6.	Wydajność grafiki	Grafika zintegrowana z procesorem powinna umożliwiać pracę min. dwumonitorową, współdzielona i dynamicznie przydzielana pamięć z RAM.	
7.	Matryca	Rozmiar matrycy / plamki	min.21.5" / max. 0,24mm
		Rozdzielczość	FHD (1920x1080)
		Jasność typowa	min. 250 cd/m ²
		Kontrast typowy	700:1
		Barwa koloru (typowa)	72% NTSC
		Kąty widzenia	178 (+/- 89)
		Rodzaj matrycy	Matowa IPS
8.	Wypożażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki min. 2W na kanał. Wbudowana w obudowę matrycy cyfrowa kamera 2,0 MP z diodą LED informującą użytkownika o pracy. Mechanicznie chowana w obudowie (nie dopuszcza się kamer przykręcanych i wystających poza obrys obudowy). Wbudowany w obudowę mikrofon.	
9.	Obudowa	Typu All-in-One zintegrowana z monitorem min. 21,5". Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczeko w obudowie do założenia kłódki), Demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi. Komputer musi posiadać możliwość zainstalowania na ścianie przy wykorzystaniu ściennego systemu montażowego VESA 100. Zasilacz zewnętrzny o mocy max. 130W. Wbudowany w obudowie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System musi zapisywać logi zdarzeń w BIOS. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji. Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz wpisany na stałe w BIOS. Podstawa jednostki typu All – in – One musi umożliwiać: a) Regulację pochyłu pionowego w zakresie od -5 do 30 stopni. b) Regulację wysokości w zakresie minimum 10 cm. c) Ustawienie jednostki w trybie Pivot. d) Obrót podstawy w lewą oraz prawą stronę.	
10.	Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzającego certyfikację). Zainstalowane system operacyjny zgodnie z wytycznymi z punktu 6.5.	
11.	Bezpieczeństwo	Płyta główna zawierająca układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot'owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, Internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego. Czujnik otwarcia obudowy, musi zbierać zdarzenia i zapisywać je w BIOS.	
12.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu.	
13.	BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego	

		<p>komputera. Pełna obsługa BIOS za pomocą myszy. (przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury).</p> <p>Informacje dostępne z poziomu BIOS na potrzeby inwentaryzacji: wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach, procesor (typ, nazwa, typowa prędkość, minimalna, maksymalna, cache L2 i L3) , pojemności zainstalowanego lub zainstalowanych dysków twardej MAC adres zintegrowanej karty sieciowej, zintegrowany układ graficzny, kontroler audio.</p> <p>Informacje dostępne w samym menu BIOS bez stosowania dodatkowego oprogramowania jak i wbudowanego systemu diagnostycznego.</p> <p>Możliwość, ustawienia hasła na poziomie:</p> <ul style="list-style-type: none"> - administratora [hasło nadrzędne] - użytkownika/systemowego [hasło umożliwiające użytkownikowi zmianę swojego hasła i zgodnie z uprawnieniami nadanymi przez administratora dokonywać zmian ustawień BIOS], rozruch systemu operacyjnego [hasło blokuje start systemu operacyjnego]. <p>Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.</p> <p>Możliwość wyłączenia/włączenia karty sieciowej.</p> <p>Możliwość włączenia/wyłączenia kontrolera SATA.</p> <p>Możliwość włączenia/wyłączenia kontrolera audio.</p> <p>Możliwość włączenia/wyłączenia układu TPM.</p> <p>Możliwość włączenia/wyłączenia wbudowanej kamery i czytnika kart multimedialnych.</p> <p>Możliwość włączenia/wyłączenia czujnika otwarcia obudowy, ustawienia go w tryb cichy.</p> <p>Możliwość przypisania w BIOS numeru nadawanego przez Administratora oraz możliwości weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym. [musi umożliwiać znaki specjalne (@#\$%^)].</p> <p>Możliwość zdefiniowania automatycznego uruchamiania komputera w min. dwóch trybach: codziennie lub w wybrane dni tygodnia.</p> <p>Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.</p> <p>Możliwość wyłączania portów USB w szczególności pojedynczo w dowolnej kombinacja.</p> <p>BIOS musi nanosić automatycznie wszystkie zmiany konfiguracji dotyczące w szczególności: pamięci, procesora, dysku.</p>
14.	Certyfikaty i standardy	<p>Urządzenia muszą być wyprodukowane zgodnie z norą ISO 9001 oraz 50001 (certyfikaty załączyć do oferty).</p> <p>Deklaracja zgodności CE (załączyć do oferty).</p> <p>Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram</p> <p>Certyfikat TCO – do oferty załączyć certyfikat lub wydruk ze strony http://tcocertified.com/product-finder/</p>
15.	Ergonomia	<p>Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy jałowej dysku twardego (IDLE) wynosząca maksymalnie 24 dB (załączyć oświadczenie producenta).</p>
16.	System Operacyjny	<p>Zainstalowany system operacyjny Windows 10 Professional w wersji edukacyjnej, klucz licencyjny zapisany trwale w BIOS, umożliwiający instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. Funkcjonalność systemu jak w punkcie 5.</p>
17.	Wymagania dodatkowe	<p>Wbudowane porty:</p> <ul style="list-style-type: none"> 1x DP++ 1.4/HDCP 2.3 port; 1x USB 3.2 Gen 2 Type-C port;

		<p>3x USB 3.2 Gen 1 Type-A port; 2x USB 2.0; Wymagane porty USB wbudowane, nie dopuszcza się stosowania rozgałęziaczy, hub'ów itp.;</p> <p>1x Universal audio jack z boku lub dołu obudowy; 1x One Line-out audio; 1x RJ-45 port 10/100/1000 Mbps; Czytnik kart SD min. 3.0; Karta WiFi ac+ bluetooth 5.</p> <p>Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, min. 1 złącza M.2 2280 dla dysku twardego oraz 1 złącze M.2 karty WiFi.</p> <p>Klawiatura USB w układzie polski programisty. Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll). Wbudowany napęd DVD RW.</p>
18.	Dodatkowe oprogramowanie	<p>Oprogramowanie producenta komputera z nieograniczoną czasowo licencją na użytkowanie umożliwiające:</p> <ul style="list-style-type: none"> - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji; - sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi; - dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne; - włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji; - sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania); - dostęp do wykazu wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml; - dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku *.xml; <p>Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku. W ofercie należy podać nazwę oprogramowania.</p>
19.	Wsparcie techniczne	<p>Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.</p> <p>Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego)</p>
20.	Warunki gwarancja	<p>Gwarancja 36 miesięcy, producenta, świadczona na miejscu u klienta. Czas reakcji serwisu – do końca następnego dnia roboczego.</p> <p>Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.</p> <p>Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – oświadczenia Producenta potwierdzające, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta wymagane będzie przed podpisaniem umowy. Oświadczenie producenta</p>

		komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem – wymagane będzie przed podpisaniem umowy.
--	--	--

5. Wymagania minimalne dla systemów operacyjnych zainstalowanych na komputerach All-In-One oraz komputerach przenośnych – 140 szt.

Lp.	Nazwa	Wymagane minimalne parametry techniczne.
1.	System operacyjny	<p>System musi być zainstalowany na komputerach z punktu 1, 2 i 4 (przez producenta lub Wykonawcę).</p> <p>Klucz licencyjny zapisany trwale w BIOS, umożliwiający instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.</p> <p>System operacyjny Windows 10 Professional 64-bit w języku polskim, fabrycznie nowy, nigdy wcześniej nieaktywowany na innego użytkownika lub równoważny*.</p> <p>*Zamawiający przez równoważność rozumie (min. parametry):</p> <p>System operacyjny klasy desktop musi spełniać następujące min. wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:</p> <ul style="list-style-type: none"> • Interfejs graficzny użytkownika pozwalający na obsługę: <ul style="list-style-type: none"> - klasyczną przy pomocy klawiatury i myszy, - dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. • Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim. • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimedialny, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe. • Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje. • Wbudowany system pomocy w języku polskim. • Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. • Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego. • Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika. • Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta z mechanizmem sprawdzającym, które z poprawek są potrzebne. • Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. • Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego, • Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. • Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). • Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. • Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących, lub ograniczających funkcjonalność systemu lub aplikacji.

		<ul style="list-style-type: none"> • Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. • Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe. • Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. • Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu. • 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. • Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. • Obsługa 12standard NFC (near field communication). • Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). • Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. • Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. • Mechanizmy uwierzytelniania w oparciu o: <ul style="list-style-type: none"> - login i hasło, - karty z certyfikatami (smartcard), - wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), - wirtualnej tożsamości użytkownika potwierdzanej za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu. Mechanizm musi być ze specyfikacją FIDO. • Mechanizmy wieloskładnikowego uwierzytelniania. • Wsparcie dla uwierzytelniania na bazie Kerberos v. 5. • Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu. • Wsparcie dla algorytmów Suite B (RFC 4869). • Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji. • Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku. • Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym. • Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny. • Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol 2.0. • Możliwość selektywnego usuwania konfiguracji oraz danych określonych, jako dane organizacji. • Możliwość konfiguracji trybu „kioskowego” dającego dostęp tylko do wybranych aplikacji i funkcji systemu. • Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej Ipsec.
--	--	--

		<ul style="list-style-type: none"> • Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. • Wsparcie dla środowisk Java i NET Framework 4.X – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. • Wsparcie dla Jscript i VBScript – możliwość uruchamiania interpretera poleceń. • Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. • Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego. (provisioning). • Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. • Rozwiązanie ma umożliwiać wdrożenie nowego obrazu poprzez zdalną instalację. • Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. Quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. • Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. • Udostępnianie wbudowanego modemu. • Oprogramowanie dla tworzenia kopii zapasowych (Backup) - automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. • Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. • 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.). • Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). • Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych. • Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika. • Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module). • Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych. • Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. • Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
--	--	---

6. Licencja CISCO L-AC-PLS-3Y-S1 Cisco AnyConnect Plus License, 1 User for 3 Year (25-99 Users level) – eDelivery – 2x50 szt.

Z tytułu posiadania przez Zamawiającego sprzętu firmy Cisco Zamawiający nie dopuszcza możliwości zaoferowania oprogramowania równoważnego. Min. czas ważności licencji na zakupione oprogramowanie to 36 miesięcy.

7. Pakiet biurowy – 90 szt.

Lp.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Pakiet biurowy	<p>Pakiet biurowy z interfejsem i słownikiem w języku polskim Microsoft Office 2021 H&B - licencja wieczysta (z nośnikiem i/lub licencją elektroniczną), fabrycznie nowy, pozwalający na używanie oprogramowania na jednym komputerze PC lub Mac, nigdy wcześniej nieaktywowany na innego użytkownika lub równoważny*.</p> <p>Zamawiający nie dopuszcza licencji subskrypcyjnych.</p> <p>*Zamawiający przez równoważność rozumie: Zintegrowany pakiet aplikacji biurowych, w którego skład ma wchodzić min.:</p> <ul style="list-style-type: none"> • Edytor tekstów. • Arkusz kalkulacyjny. • Narzędzie do przygotowania i prowadzenia prezentacji. • Narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami). • Pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. • Powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim. • Dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach od 8-16 – cena połączenia nie większa niż cena połączenia lokalnego. • Publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa, co najmniej 5 lat od daty zakupu. • Możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (min. WCAG 2.0). <p>Edytor tekstów musi umożliwiać:</p> <ul style="list-style-type: none"> • Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. • Wstawianie oraz formatowanie tabel. • Wstawianie oraz formatowanie obiektów graficznych. • Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). • Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. • Automatyczne tworzenie spisów treści. • Formatowanie nagłówków i stopek stron. • Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie. • Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. • Określenie układu strony (pionowa/pozioma). • Wydruk dokumentów. • Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. • Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

		<p>Arkusz kalkulacyjny musi umożliwiać:</p> <ul style="list-style-type: none"> • Tworzenie raportów tabelarycznych. • Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych. • Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. • Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice). • Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. • Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych. • Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. • Wyszukiwanie i zamianę danych. • Wykonywanie analiz danych przy użyciu formatowania warunkowego. • Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. • Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. • Formatowanie czasu, daty i wartości finansowych z polskim formatem. • Zapis wielu arkuszy kalkulacyjnych w jednym pliku. • Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. <p>Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:</p> <ul style="list-style-type: none"> • Przygotowywanie prezentacji multimedialnych, które mogą być prezentowane przy użyciu projektora multimedialnego. • Drukowanie w formacie umożliwiającym robienie notatek. • Zapisanie, jako prezentacja tylko do odczytu. • Nagrywanie narracji i dołączanie jej do prezentacji. • Opatrywanie slajdów notatkami dla prezentera. • Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo. • Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego. • Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym. • Możliwość tworzenia animacji obiektów i całych slajdów. • Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera. <p>Narzędzie do zarządzania informacją prywatną (poczta elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:</p> <ul style="list-style-type: none"> • Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, • Przechowywanie wiadomości na serwerze lub w lokalnym pliku stworzonym z zastosowaniem efektywnej kompresji danych. • Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców. • Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną. • Automatyczne grupowanie poczty o tym samym tytule. • Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy. • Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów. • Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie. • Zarządzanie kalendarzem. • Udostępnianie kalendarza innym użytkownikom z możliwością określania
--	--	---

		<p>uprawnień użytkowników.</p> <ul style="list-style-type: none"> • Przeglądanie kalendarza innych użytkowników. • Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach. • Zarządzanie listą zadań. • Zlecanie zadań innym użytkownikom. • Zarządzanie listą kontaktów. • Udostępnianie listy kontaktów innym użytkownikom. • Przeglądanie listy kontaktów innych użytkowników. • Możliwość przesyłania kontaktów innym.
--	--	--

8. Tablet 10" – 40 szt.

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Typ	Tablet przenośny o przekątnej ekranu minimum 10,5" z modemem LTE.
2.	Procesor	Minimum ośmiordzeniowy.
3.	Ekran	Dotykowy TFT o rozdzielczości min. 1920 x 1200 oraz o przekątnej ekranu min. 10,5", obsługujący 16M kolorów.
4.	Dźwięk	Min. 4 głośniki, co najmniej jedno złącze minijack 3,5mm.
5.	Kamery	Przednia min. 5 MP, Tylna min. 8 MP.
6.	Obsługiwane standardy sieci GSM	<p>Wymagania minimalne:</p> <ul style="list-style-type: none"> • 2G GSM; GSM850, GSM900, DCS1800, PCS1900. • 3G UMTS; B1(2100), B2(1900), B4(AWS), B5(850), B8(900) • 4G FDD LTE; B1(2100), B2(1900), B3(1800), B4(AWS), B5(850), B7(2600), B8(900), B12(700), B17(700), B20(800), B28(700), B66(AWS-3). • 4G TDD LTE; B38(2600), B40(2300), B41(2500) .
7.	Pamięć Ram	Min. 4 GB.
8.	Pamięć wewnętrzna	Min. 64 GB.
9.	Porty	<p>Wymagania minimalne:</p> <ul style="list-style-type: none"> • 1 x 3,5 mm minijack; • 1 x USB (Type C); • Czytnik kart pamięci microSD; • Gniazdo kart Sim w wersji Nano.
10.	Obsługiwane standardy SD	<p>Wymagania minimalne:</p> <ul style="list-style-type: none"> • SD; • SDHC; • SDXC.
11.	Komunikacja	<p>Wymagania minimalne:</p> <ul style="list-style-type: none"> • Wi-Fi, 802.11 a/b/g/n/ac 2.4G+5GHz, VHT80; • Wi-Fi Direct; • Bluetooth v5.0.
12.	Waga	Max. 600g

13.	Bateria	Min. 7000 mAh LI-ion, wsparcie szybkiego ładowania o mocy min. 15W
14.	System operacyjny	Android, zainstalowany na urządzeniu z możliwością wsparcia min. 24 miesiące.
15.	Warunki gwarancji	Min. 24 miesiące w trybie Door to door.

9. Przełączniki sieciowe – 3 szt.

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Typ/Opis	<ul style="list-style-type: none"> Zarządzany przełącznik warstwy min. 3 ISO OSI. Zaoferowane urządzenia muszą mieć możliwość połączenia w niezależny stos w oparciu o protokół VTP, widziany z perspektywy sieci jako jedno urządzenie. Wraz z przełącznikami należy dostarczyć wszystkie komponenty wymagane do ich połączenia w stos (np. okablowanie, licencje).
2.	Obudowa	<ul style="list-style-type: none"> Urządzenie musi być przystosowane do montażu w szafie stelażowej 19”. Wraz z urządzeniem muszą być dostarczone niezbędne elementy do montażu w szafie stelażowej. Wysokość urządzenia: maksymalnie 1U. Urządzenie posiada, co najmniej następujące diody statusowe: działanie urządzenia, działanie wbudowanych portów Ethernet.
3.	Interfejsy	<ul style="list-style-type: none"> Co najmniej 24 zabudowane w urządzeniu gniazda 10Base-T/100Base-TX/1000Base-T automatycznie rozpoznające kable proste / krzyżowe oraz wspierające automatyczną negocjację prędkości, duplex. Porty muszą obsługiwać funkcjonalność zasilania PoE+. Zabudowany w urządzeniu port konsoli lokalnej w standardzie RS232 zakończony gniazdem RJ-45 lub inny (w przypadku innego portu konsoli niezbędne jest dostarczenie wymaganego okablowania/przejsiówki). Urządzenie posiada możliwość montażu, co najmniej czterech interfejsów (modułów) w standardzie SFP+ o przepustowości minimum 1Gbit z możliwością obsadzenia modułami minimum 1000Base-SX, 1000Base-LX/LH.
4.	Zasilanie	<p>Przełącznik musi posiadać minimum jeden wymienny zasilacz AC 230V o maksymalnej mocy nie przekraczającej łącznie 715W.</p> <p>Urządzenie dostarczane wraz ze standardowym kablem zasilającym o długości co najmniej 1,5m z wtykiem CEE7/7.</p>
5.	Architektura	<p>Przełącznik musi zapewniać możliwość budowania stosu urządzeń z zapewnieniem następujących parametrów:</p> <ul style="list-style-type: none"> przepustowość w ramach stosu min. 320Gb/s; minimum 8 urządzeń w stosie; stos widoczny jako jeden węzeł sieciowy dla procesu spanning-tree; zarządzanie poprzez jeden adres IP; możliwość tworzenia połączeń cross-stack link aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z 802.3ad. <p>Przełącznik musi być wyposażony w redundantne moduły wentylatorów.</p>
6.	Wydajność	<p>Przełącznik musi posiadać minimum 16MB bufor pamięci współdzielony przez wszystkie porty.</p> <p>Przełącznik musi posiadać minimum 8GB pamięci DRAM i 16GB pamięci flash.</p> <p>Przełącznik musi zapewniać przepustowość nie mniejszą niż 56Gbps.</p> <p>Szybkość przełączania przełącznika musi wynosić minimum 41Mpps.</p> <p>Obsługa minimum:</p> <ul style="list-style-type: none"> 4096 sieci VLAN; 1000 wirtualnych interfejsów sieciowych SVI; 32000 adresów MAC; 32000 tras IPv4; 16000 tras IPv6.
7.	Oprogramowanie/	Obsługa protokołu NTP.

	Funkcjonalność	<p>Obsługa IGMPv1/2/3.</p> <p>Wszystkie porty na przełączniku muszą obsługiwać standard 802.1AE (szyfrowanie ruchu) 128-bit.</p> <p>System operacyjny przełącznika jest konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz umożliwia eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów.</p> <p>Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:</p> <ul style="list-style-type: none"> • IEEE 802.1w Rapid Spanning Tree; • Per-VLAN Rapid Spanning Tree (PVRST+); • IEEE 802.1s Multi-Instance Spanning Tree; • Obsługa minimum 128 instancji protokołu STP. <p>Obsługa protokołu IEEE 802.1ab LLDP i LLDP-MED.</p> <p>Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.</p> <p>Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP.</p> <p>Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:</p> <ul style="list-style-type: none"> • minimum 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level); • autoryzacja użytkowników sieci w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN; • autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL; • możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC; • wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem; • możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176; • minimum 1600 wpisów dla list kontroli dostępu (ACE); • funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www); • obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard; • zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard); • możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+; • obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia). <p>Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:</p> <ul style="list-style-type: none"> • implementacja co najmniej 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi; • implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek; • możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority); • klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie
--	----------------	--

		<p>następujących parametrów: źródłowy/docelowy adres MAC źródłowy/docelowy adres IP, źródłowy/docelowy port TCP;</p> <ul style="list-style-type: none"> • możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting). Możliwość skonfigurowania do 1000 ograniczeń per przełącznik; • kontrola sztormów dla ruchu broadcast/multicast/unicast; • możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP. <p>Urządzenie musi zapewniać możliwość routingu statycznego i dynamicznego dla IPv4 i IPv6. Urządzenie musi zapewniać wsparcie minimum dla protokołów routingu IPv4 (OSPF, RIP), funkcjonalności Policy-based routingu i routingu multicast.</p>
8.	Zarządzanie i konfiguracja	<p>Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN).</p> <p>Urządzenie musi zapewniać możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 16.000. Wymagane jest sprzętowe wsparcie dla gromadzenia statystyk NetFlow/J-Flow.</p> <p>Dedykowany port umożliwiający dostęp do linii poleceń (CLI).</p> <p>Minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB.</p> <p>Urządzenie musi być wyposażone w port konsoli USB.</p> <p>Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją.</p> <p>Urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.</p> <p>Urządzenie musi posiadać wbudowany analizator pakietów.</p> <p>Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6.</p> <p>Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych.</p>
9.	Gwarancja i serwis	<p>Wymagane jest, aby przełącznik był objęty wsparciem producenta na okres minimum 36 miesięcy od daty dostawy w reżimie minimum 8x5xNBD. Wsparcie musi obejmować naprawy sprzętu, aktualizacje oprogramowania przełącznika oraz dostęp do pomocy technicznej producenta.</p>
10.	Instalacja/ Konfiguracja	<p>Przełączniki muszą zostać dostarczone z zainstalowanym najnowszym oprogramowaniem systemowym producenta.</p>

10. Serwer rackowy – 1 szt.

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Obudowa	<ul style="list-style-type: none"> • Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia). • Obudowa serwera musi umożliwiać min. 12 dysków typu Hot Swap, SAS/SATA/SSD,

		<p>3,5".</p> <ul style="list-style-type: none"> Szyny montażowe muszą być kompatybilne z szafą serwerową Zamawiającego Dell Netshelter SX 42U. Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/WiFi.
2.	Płyta główna	Płyta główna z możliwością zainstalowania min. dwóch procesorów klasy serwerowej.
3.	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych.
4.	Procesor	Zainstalowane min. dwa procesory ośmiordzeniowe klasy x86 – 64 bity, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 131 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocessorowej. Do oferty należy załączyć wydruk ze strony potwierdzający osiągnięty wynik dla oferowanego modelu serwera.
5.	Pamięć operacyjna	<ul style="list-style-type: none"> Min. 256 GB RDIMM DDR4 3200MT/s w modułach o pojemności min. 64GB każdy. Płyta główna musi posiadać min. 32 sloty na pamięć i umożliwiać rozbudowę do minimum 8TB RDIMM pamięci. Obsługa zabezpieczeń i funkcjonalności, min: Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing.
6.	Gniazda PCI	<p>Serwer musi posiadać minimum 8 slotów PCI-Express Generacji 4, w tym:</p> <ul style="list-style-type: none"> Minimum 2 sloty PCI-Express Generacji 4 działający z prędkością x16.
7.	Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> Minimum 4 wbudowane porty 1 Gb Ethernet BaseT, które nie zajmują gniazd PCIe. Min. wbudowane lub zainstalowane 4 porty obsługujące prędkości 10Gb Ethernet BaseT. Min. wbudowane lub zainstalowane 2 porty obsługujące prędkości 10Gb Ethernet SFP+.
8.	Dyski twarde	<p>Zainstalowane dyski:</p> <ul style="list-style-type: none"> Min. 2x480GB M.2 SATA Hot-Plug z możliwością konfiguracji RAID 1. Min. 8x 4TB SATA 6Gb/s, Hot-Plug. <p>Możliwość instalacji dysków SFF SAS/SATA/SSD, 2,5" lub 3,5.</p> <p>Zainstalowany dedykowany moduł dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 16GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.</p>
9.	Kontroler RAID	<p>Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID min.: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.</p> <p>Dodatkowy sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID min.: 0, 1, 5, 6, 10, 50, 60, wyposażony w zewnętrzne porty umożliwiające podłączenie do serwera półki dyskowej.</p>
10.	Porty	<p>5x USB, w tym min. 2 porty USB 3.0;</p> <p>1 port VGA;</p> <p>Możliwość rozbudowy o Serial Port.</p>
11.	Karta graficzna	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024.

12.	Chłodzenie	<ul style="list-style-type: none"> Zestaw wentylatorów redundantnych typu hot-plug. Możliwość skonfigurowania serwera do pracy w temperaturze otoczenia 45st.C, tak, żeby zapewnić zgodność ze standardem ASHRAE Class A4.
13.	Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1400W.
14.	System operacyjny/ dodatkowe oprogramowanie	Zainstalowany na serwerze, zgodny z wymogami z punktu 11.
15.	Bezpieczeństwo	<ul style="list-style-type: none"> Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.
16.	Diagnostyka	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlanie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
17.	Karta/ Moduł zarządzający/ Dodatkowe oprogramowanie	<p>Rozwiązanie sprzętowe (tzn. Moduł), niezależne od systemów operacyjnych, zintegrowane z płytą główną lub montowane niezależnie na płycie głównej, nieograniczające w żaden sposób dostępnych wymaganych portów/slotów w zaferowanym Serwerze, posiadające dedykowany port RJ45 i umożliwiające:</p> <ul style="list-style-type: none"> zdalny dostęp do graficznego interfejsu Web karty zarządzającej; zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; możliwość podmontowania zdalnych wirtualnych napędów; wirtualną konsolę z dostępem do myszy, klawiatury; wsparcie dla IPv6; wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; integracja z Active Directory; możliwość obsługi przez dwóch administratorów jednocześnie; wsparcie dla dynamic DNS; wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera. <p>Moduł zarządzania zdalnego, musi udostępniać wbudowane narzędzie wspomagające instalację systemów operacyjnych oraz konfigurację serwera. Narzędzie dostępne z poziomu BIOS poprzez interfejs graficzny (GUI), udostępniające minimum następujące funkcjonalności:</p>

		<ul style="list-style-type: none"> Wspomaganą instalację systemu operacyjnego – wybór najlepszych sterowników i firmware. Diagnostykę wszystkich elementów sprzętowych serwera. Konfigurację kontrolera macierzowego i dysków poprzez GUI. Ustawienia parametrów BIOS.
18.	Certyfikaty	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklarację CE.</p> <p>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.</p>
19.	Warunki gwarancji	<p>Minimum 36 miesięcy gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p> <p>Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzację producenta oferowanego serwera – dokumenty potwierdzające należy załączyć do oferty.</p> <p>Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p> <p>Możliwość rozszerzenia gwarancji przez producenta do 7 lat.</p> <p>Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem – wymagane będzie przed podpisaniem umowy.</p> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.</p>
20.	Instalacja i konfiguracja	<ul style="list-style-type: none"> Instalacja dostarczonego serwera we wskazanej przez Zamawiającego szafie rack Dell Netshelter SX 42U. Instalacja systemu operacyjnego (system również może być preinstalowany przez Producenta). Instalacja RAID na dyskach: RAID-1 i RAID-10. Instalacja dostarczonych modułów SFP+ (w razie konieczności).
21.	Dokumentacja użytkownika	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>

11. System operacyjny serwerowy – 1 szt.

Lp.	Nazwa	Wymagane minimalne parametry techniczne.
1.	System operacyjny	<p>System musi być zainstalowany na serwerze z punktu 10 (przez producenta lub Wykonawcę).</p> <p>Windows Server Data Center Core 2022 MOLP GOV– fabrycznie nowy, nigdy wcześniej nieaktywowany na innego użytkownika z nośnikiem i/lub licencją elektroniczną, wraz z systemem należy dostarczyć wymaganą ilość licencji (na każdy z rdzeni oferowanego procesora dla serwera z punktu 11). Zainstalowany na dostarczonym serwerze przez Wykonawcę/Producenta – lub równoważny*. System na nośniku danych</p> <p>*Przez równoważność zamawiający rozumie (min. parametry):</p> <ul style="list-style-type: none"> Możliwość wykorzystania 512 logicznych procesorów oraz co najmniej 24 TB

		<p>pamięci RAM w środowisku fizycznym.</p> <ul style="list-style-type: none"> • Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. • Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. • 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. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. • Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy, jakości przeprowadzone przez producenta systemu operacyjnego. • Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. • Wbudowane wsparcie instalacji i pracy na wolumenach, które: <ul style="list-style-type: none"> - pozwalają na zmianę rozmiaru w czasie pracy systemu, - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje i folderów, - umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, - umożliwiają zdefiniowanie list kontroli dostępu (ACL). • Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. • Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. • Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET. • Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. • Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. • Dostępne dwa rodzaje graficznego interfejsu użytkownika: <ul style="list-style-type: none"> - klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, - dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. • Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. • Mechanizmy logowania w oparciu o: <ul style="list-style-type: none"> - login i hasło, - karty z certyfikatami (smartcard), - wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). • 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. • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
--	--	--

	<ul style="list-style-type: none"> • Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. • Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. • Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). • Wsparcie dla środowisk Java i .NET Framework 4.x - możliwość uruchomienia aplikacji działających we wskazanych środowiskach. • Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: <ul style="list-style-type: none"> - podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, - 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: <ul style="list-style-type: none"> ✓ 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. - Zdalna dystrybucja oprogramowania na stacje robocze. - Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej - Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: <ul style="list-style-type: none"> ✓ 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. - szyfrowanie plików i folderów, - szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), - możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, - Serwis udostępniania stron WWW. • Wsparcie dla protokołu IP w wersjach 4 oraz 6 (IPv4; IPv6). Wsparcie dla algorytmów Suite B (RFC 4869). • Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows. • 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: <ul style="list-style-type: none"> • Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
--	--

		<ul style="list-style-type: none"> - 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). <ul style="list-style-type: none"> • 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. • Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). • Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. • Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. • Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. • Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. <p>System musi współpracować z posiadanymi i wdrożonymi przez Zamawiającego w pełni usługami: min. Active Directory, DNS, DHCP. Zamawiający posiada wymagane licencje dostępowe MS CAL 2022.</p> <p>System musi być zainstalowany na serwerze zaoferowanych z punktu 6.10. „Serwer rakowy – 1 szt.”.</p>
--	--	---

12. Macierz dyskowa – 1 szt.

Lp.	Nazwa	Wymagane minimalne parametry techniczne
1.	Konfiguracja obudowy	Umożliwiająca zamontowanie min. 12 dysków 3,5 cala SAS, NL-SAS, lub 2,5" SSD, wysokość maksymalna 2U, obudowa typu RACK.
2.	Kontrolery	<p>Kontroler RAID ze wsparciem funkcjonalności multi-pathing posiadający łącznie minimum:</p> <ol style="list-style-type: none"> 1) Min. dwa porty optyczne 10Gb (iSCSI) do podłączenia serwerów. 2) Min. dwa porty sieciowe 10Gb (iSCSI) w standardzie Base-T (RJ45). <p>Zamawiający dopuszcza zastosowanie czterech portów optycznych 10Gb (iSCSI) oraz osiągnięcie dwóch portów w standardzie Base-T (RJ45) za pomocą dodatkowych wkładek konwertujących porty optyczne na Base-T (RJ45), pod warunkiem ich dostarczenia wraz z urządzeniem.</p> <p>Możliwość skonfigurowania różnych stopni ochrony, co najmniej RAID: 0, 1, 5, 6 i 10 lub DDP (Dynamic Disk Pools) dla ochrony danych i zapewnienia wydajności systemu.</p> <p>Liczba możliwych hostów do podłączenia: min. 250</p> <p>Minimalna ilość wolumenów: 500</p> <p>Minimalna liczba kopii Snapshot: 500</p> <p>Minimalna liczba możliwych par replikowanych woluminów: 30.</p>
3.	Bezpieczeństwo	Macierz wyposażona min. w dwa redundantne zasilacze oraz min. dwa redundantne wentylatory, umożliwiające wymianę w trybie „hot-swap”.
4.	Dyski twarde	Min. Hot-Plug 4TB 7.2k NLSAS 3.5 cala – 12 sztuk.
5.	Rozbudowa	Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do minimum 96 dysków łącznie.
6.	Zasilanie	Dwa redundantne zasilacze z możliwością wymiany („hot-swap”).
7.	Elementy montażowe	Szyny umożliwiające montaż macierzy w posiadanej szafie serwerowej przez Zamawiającego.

8.	Oprogramowanie/ pozostałe wymogi	<p>Macierz dyskowa musi gwarantować pracę z przepustowością min. 1220 Mb/s dla zapisu, min. 240 Mb/s dla jednoczesnego odczytu oraz min. 800 jednoczesnych sesji iSCSI na kontroler.</p> <p>Zarządzanie macierzą poprzez minimum oprogramowanie zarządzające lub przeglądarkę internetową, umożliwiające konfigurację poszczególnych funkcji macierzy oraz powiadamiania o awarii.</p> <p>Minimum pełna obsługa protokołu SNMP P z obsługą baz MIB-II. W przypadku awarii komponentów SNMP, możliwość wygenerowania alarmowych wiadomości co najmniej na e-mail. Ponadto możliwość generowane i wysyłane komunikatów AutoSupport.</p> <p>Musi pozwalać na monitorowanie i wykrywanie potencjalnych awarii dysków, zanim spowodują one problem oraz pozwalać na automatyczne przełączanie awaryjne, wykrywanie i rekonstrukcję napędów w przypadku zastosowania globalnych dysków wymienianych w czasie prac.</p> <p>Oprogramowanie do zarządzania pamięcią masową musi być wyposażone co najmniej w funkcję dynamicznej konfiguracji, która musi umożliwić min. na rozbudowę, zmianę konfiguracji i konserwację macierzy w czasie pracy bez przerywania operacji we-wy systemu pamięci masowej.</p>
9.	Gwarancja na cały zestaw	<p>Min. 36 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z maks. reakcją w następnym dniu roboczym tzw. Next Business Day (NBD). Możliwość rozszerzenia (dodatkowo odpłatnie) gwarancji przez producenta do min. 60 miesięcy (5 lat), oraz o następujące opcje:</p> <ol style="list-style-type: none"> 1. W przypadku awarii dyski twarde pozostają własnością Zamawiającego. 2. Diagnostyka usterki przeprowadzana na miejscu w siedzibie klienta. 3. Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu. 4. Reakcja serwisu na zgłoszoną usterkę skrócona do 4 godzin.
10.	Waga	Do 30 kg, bez uwzględnienia rozbudowy z pozycji 5.
13.	Normy	Macierz zgodna z normą min. ENERGY STAR Data Center Storage (z uwzględnieniem rozbudowy z pozycji 6) .
14.	Warunki pracy	Min. temperatura otoczenia (przy pracy) do +40°C.
15.	Wsparcie dla systemów operacyjnych	Min. Microsoft Windows Server, Red Hat Enterprise Linux, Novell SUSE Linux Enterprise Server, Apple Mac OS, Oracle Solaris, HPE HP-UX, CentOS Linux, Oracle Enterprise Linux, IBM AIX, VMware ESX.
16.	Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
17.	Certyfikaty	Macierz musi być wyprodukowana zgodnie z normą min. ISO 9001 oraz EN 29001.

13. Network Intrusion Prevention System (NIPS) – 1 szt.

Lp.	Nazwa	Wymagane minimalne parametry techniczne.
1.	Przepustowość	Min. 4Gb/s (IPS).
2.	Liczba portów	Min. 4 szt. Gigabit Ethernet (wbudowane) oraz posiadać min. jedno gniazdo dla modułów rozszerzeń pozwalające na uzyskanie min. 4 portów Gigabit Ethernet lub 4 portów SFP (możliwe do uzyskania poprzez zastosowanie wkładek).
3.	Usługi sieciowe	Proponowane rozwiązanie musi być w stanie pracować jednocześnie w trybie warstwy 3 (routing), trybie online (most) i warstwie 2 (kopia ruchu) (bez konieczności wirtualizacji sprzętu).
4.	Kontrola aplikacji	<ul style="list-style-type: none"> • Rozwiązanie powinno obsługiwać identyfikację IP hostów, ilość endpointów, czas online, czas offline. • Rozwiązanie musi obsługiwać ponad 4700 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka.

		<ul style="list-style-type: none"> Rozwiązanie musi rozpoznawać aplikacje wykorzystujące IPv6. Rozwiązanie musi obsługiwać identyfikację aplikacji dla ruchu szyfrowanego SSL. Rozwiązanie musi wspierać identyfikację aplikacji mobilnych na Androida i iOS. Rozwiązanie powinno obsługiwać wyświetlanie opisu, czynników ryzyka, zależności, typowych używanych portów i adresów URL dla dodatkowych odwołań i informacji dla każdej aplikacji w interfejsie WebUI. Rozwiązanie musi obsługiwać blokowanie, ponowne uruchamianie sesji, monitorowanie i kształtowanie ruchu dla aplikacji. Rozwiązanie musi być w stanie identyfikować i kontrolować aplikacje w chmurze, musi zapewniać wielowymiarowe monitorowanie i statystyki dla aplikacji w chmurze, w tym kategorię ryzyka i funkcje.
5.	Porty USB	Min. 2 szt.
6.	Ochrona przed zagrożeniami	<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać ponad 15000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, automatyczne wstawianie lub wyodrębnianie sygnatur oraz zintegrowaną encyklopedię zagrożeń. Rozwiązanie musi obsługiwać zapobieganie włamaniom dla ruchu szyfrowanego SSL. Rozwiązanie musi obsługiwać ochronę środowiska IPV6. Rozwiązanie musi obsługiwać ochronę przed sql injection, CC i atakom XSS. Rozwiązanie musi obsługiwać sprawdzanie linków zewnętrznych. Rozwiązanie powinno obsługiwać ochronę przed atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, metodami przyjaznymi dla robotów. Wspierane powinny być 4 metody uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA Rozwiązanie powinno obsługiwać wykrywanie anomalii protokołu, wykrywanie oparte na prędkości. Rozwiązanie musi obsługiwać następujące akcje IPS: domyślne, monitorowanie, blokowanie, resetowanie (adres IP atakujących lub IP ofiary, interfejs wejściowy) z czasem wygaśnięcia Rozwiązanie musi obsługiwać opcję logowania pakietów. Rozwiązanie musi obsługiwać profil zabezpieczeń IPS na podstawie ważności, obiektu docelowego, systemu operacyjnego, aplikacji lub protokołu. Rozwiązanie musi obsługiwać zapobieganie włamaniom dla protokołów HTTP, SMTP, IMAP. POP3, VOIP, NETBIOS itp. Rozwiązanie musi wspierać weryfikację protokołów http typu Get, Head, Put, Post. Rozwiązanie musi obsługiwać wyłączenie IP z określonych sygnatur IPS. Rozwiązanie musi obsługiwać tryb działania sniffera IDS. Rozwiązanie musi obsługiwać predefiniowaną konfigurację profili IPS. Rozwiązanie musi obsługiwać tworzenie zdefiniowanych przez użytkownika sygnatur IPS. Proponowane rozwiązanie musi obsługiwać wykrywanie reputacji IP i blokowanie adresów IP serwera botnetów za pomocą globalnej bazy danych reputacji IP. Proponowane rozwiązanie powinno wspierać szczegółowy opis predefiniowanych profili IPS. Rozwiązanie musi obsługiwać rejestrację zagrożeń IPv6: obsługa przechwytywania i pobierania pakietów IPv6 Szczegóły zagrożeń muszą obsługiwać identyfikator URI i dekodowanie danych ataków Obsługa wykrywania anomalii protokołów HTTP/DNS/FTP/MSRPC/POP3/SMTP/SUNRPC i Telnet

		<ul style="list-style-type: none"> • Obsługa inspekcji Reverse Shell • Blokowanie plików po rozszerzeniu dla minimum 100 typów plików • Rozwiązanie musi wykrywać i blokować wrażliwe zdefiniowane informacje w przesyłanych plikach dla minimum doc/docx, xls/xlsx, ppt/pptx, txt w protokołach HTTP, FTP, SMTP, POP3, IMAP, SMB • Ochrona i wykrywanie skanowania protokołów IP oraz UDP • Rozwiązanie musi mieć możliwość inspekcji payloadu w ramach MPLS.
7.	Zabezpieczenia	<ul style="list-style-type: none"> • Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA). • Obudowa musi być wykonana z metalu. Ze względu na różne warunki, w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej.
8.	Antywirus	<ul style="list-style-type: none"> • Rozwiązanie musi obsługiwać ponad 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur. • Rozwiązanie musi obsługiwać antywirus oparty na przepływie dla protokołów HTTP, SMTP, POP3, IMAP, FTP/SFTP, SMB. • Rozwiązanie powinno obsługiwać wykrywanie wirusów dla skompresowanych plików, takich jak RAR, ZIP, GZIP, BZIP2, TAR; obsługa wielowarstwowego wykrywania skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji. • Rozwiązanie musi obsługiwać akcje niestandardowe dla zaszyfrowanych plików skompresowanych. • Rozwiązanie musi obsługiwać co najmniej 3 działania: fill magic, resetowanie połączenia lub logowanie tylko po wykryciu wirusa lub złośliwej strony internetowej • Rozwiązanie powinno obsługiwać ostrzeganie przed wirusami i złośliwymi stronami internetowymi, ostrzegać użytkownika, że witryna jest szkodliwą witryną lub że wykryto wirusa. • Rozwiązanie musi obsługiwać funkcje AV w środowiskach IPv6.
9.	Filtrowanie adresów URL	<ul style="list-style-type: none"> • Rozwiązanie musi obsługiwać dynamiczne filtrowanie sieci Web za pomocą chmurowej bazy danych kategoryzacji w czasie rzeczywistym: ponad 140 milionów adresów URL z co najmniej 64 kategoriami (z których nie mniej niż 8 jest związanych z bezpieczeństwem). • Rozwiązanie musi obsługiwać ręcznie zdefiniowane filtrowanie sieci Web na podstawie adresu URL, zawartości sieci Web i nagłówka MIME. • Rozwiązanie musi obsługiwać następujące dodatkowe funkcje filtrowania: <ul style="list-style-type: none"> - Aplet Java, ActiveX lub filtr plików cookie; - Blokowanie postów HTTP; - Rejestrowanie wyszukiwania słów kluczowych; - Wykluczanie ze skanowania połączeń szyfrowanych w niektórych kategoriach dla prywatności. • Rozwiązanie musi obsługiwać zastępowanie profilu filtrowania adresów URL, aby administrator mógł tymczasowo przypisać różne profile do użytkownika/grupy/adresu IP. • Rozwiązaniem powinno umożliwiać dostosowanie strony ostrzeżenia do filtrowania adresów URL.
10.	SANDBOX	<ul style="list-style-type: none"> • Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do chmury w celu analizy • Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów takich jak HTTP/HTTPS, POP3, IMAP, SMTP, FTP i SMB.

		<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR, SWF i Skryptów. Rozwiązanie musi obsługiwać kierunek transferu plików i kontrolę rozmiaru pliku. Rozwiązanie musi zawierać kompletny raport analizy zachowania złośliwych plików. Rozwiązanie powinno obsługiwać blokowanie zgodnie z wynikami wykrywania, aby szybko zablokować nieznane zagrożenie. Rozwiązanie musi obsługiwać udostępnianie globalnych informacji o zagrożeniach i blokować nieznane zagrożenia na całym świecie.
11.	Zapobieganie C&C BOTNETOM	<ul style="list-style-type: none"> Rozwiązanie musi być w stanie skutecznie wykrywać boty intranetowe i zapobiegać dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównanie uzyskanych informacji z bazą adresów C&C. Rozwiązanie musi obsługiwać regularne aktualizacje adresów serwerów botnetu. Rozwiązanie musi obsługiwać dwa typy bazy danych adresów C&C: bazę danych adresów IP (z wyłączeniem adresów IPv6) i bazę danych domen. Rozwiązanie musi obsługiwać wykrywanie protokołów TCP, HTTP i DNS. Rozwiązanie musi obsługiwać umieszczanie adresów IP i domen na białej liście. Rozwiązanie musi obsługiwać funkcjonalność DNS Sinkhole i wykrywanie tunelowania DNS.
12.	Reputacja IP	<ul style="list-style-type: none"> Obsługa filtrowania ruchu z adresów IP o niskiej reputacji, w tym botnetów, spamu, węzłów Tora, compromised, Brute-force itp. Obsługa rejestrowania, usuwania lub blokowania pakietów, jeśli złośliwy ruch dotrze do listy reputacji IP. Obsługa uaktualniania bazy danych przez zainstalowanie licencji IP Reputation. Obsługa filtrowania adresów IP botów.
13.	Ochrona przed SPAMEM	<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać klasyfikację spamu w czasie rzeczywistym i zapobieganie mu. Rozwiązanie musi obsługiwać ochronę niezależnie od języka, formatu lub zawartości wiadomości. Rozwiązanie musi obsługiwać protokoły poczty e-mail SMTP i POP3. Rozwiązanie musi obsługiwać wykrywanie zarówno ruchu przychodzącego, jak i wychodzącego. Rozwiązanie musi obsługiwać białe listy, aby umożliwić wysyłanie wiadomości e-mail z zaufanych domen. Rozwiązanie musi obsługiwać listę obejść opartą na nadawcy i niestandardowe reguły spamu. Rozwiązanie musi mieć możliwość konfiguracji czarnych i białych list dla modułu Anti-Spam.
14.	Jakość usług (QoS)	<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać maksymalną lub gwarantowaną kontrolę przepustowości dla adresów IP lub użytkowników. Rozwiązanie powinno obsługiwać tunelowanie w oparciu o domenę zabezpieczeń, interfejs, adres, pulę użytkowników/użytkowników, pulę serwer/serwer, pulę aplikacji/aplikacji, TOS, sieci VLAN. Rozwiązanie musi obsługiwać przepustowość przydzieloną w zakresie - czas, priorytet lub tę samą współdzieloną przepustowość. Rozwiązanie musi obsługiwać typ usługi (TOS) i zróżnicowane usługi (DiffServ) Rozwiązanie musi obsługiwać tworzenie zaplanowanych polityk QoS. Rozwiązanie musi obsługiwać elastyczną, priorytetową alokację pozostałej niewykorzystanej przepustowości. Rozwiązanie musi obsługiwać dwa poziomy konfiguracji ruchu, które umożliwiają

		<p>konfigurację ruchu w różnych wymiarach, takich jak użytkownicy i aplikacje. Rozwiązanie musi obsługiwać co najmniej cztery tunele na poziom, co zapewnia hierarchię kontroli ruchu.</p> <ul style="list-style-type: none"> Rozwiązanie musi obsługiwać alokację przepustowości na podstawie kategorii adresu URL. Rozwiązanie musi obsługiwać adresy IPv6 w funkcji QoS.
15.	Wysoka dostępność	<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać tryby Active/Active i Active/Passive. Rozwiązanie musi obsługiwać następujące opcje wdrażania HA: <ul style="list-style-type: none"> HA z agregacją linków; Full m; esh HA; Geograficznie rozproszony HA. Rozwiązanie musi obsługiwać funkcję bypass sprzętowych interfejsów i dedykowany interfejs HA.
16.	Administrowanie, logi i raportowanie	<ul style="list-style-type: none"> Rozwiązanie musi być obsługiwane przez WebUI i interfejs wiersza poleceń (CLI). Rozwiązanie powinno obsługiwać zarządzanie dostępem przez HTTP/HTTPS, SSH, telnet, konsolę. Rozwiązanie musi obsługiwać scentralizowane zarządzanie. Rozwiązanie musi obsługiwać uwierzytelnianie dwuskładnikowe: nazwa użytkownika/hasło, plik certyfikatu HTTPS. Rozwiązanie musi obsługiwać integrację systemu: SNMP, syslog. Rozwiązanie musi obsługiwać co najmniej 3 role administratora, w tym administratora, operatora i audytora. Rozwiązanie musi być w stanie chronić system przed atakami brute force na nazwę użytkownika i hasło. Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów. Rozwiązanie musi obsługiwać serwery Radius, AD i LDAP. Rozwiązanie musi obsługiwać szybkie wdrażanie poprzez automatyczne instalowanie z USB, uruchamianie skryptów lokalnych i zdalnych. Rozwiązanie musi obsługiwać dynamiczny dashboard w czasie rzeczywistym i szczegółowe widżety monitorowania. Urządzenie musi obsługiwać zarządzanie urządzeniami pamięci masowej: dostosowywanie i alarmowanie progu przestrzeni dyskowej, nakładanie starych danych, zatrzymywanie nagrywania ruchu. Urządzenie musi obsługiwać szczegółowe logi ruchu: przekazane, sesje naruszone, ruch lokalny, nieprawidłowe pakiety. Urządzenie musi obsługiwać pełne logi zdarzeń: audyty aktywności systemu i zarządzania, routing i sieć, VPN, uwierzytelnianie użytkowników, zdarzenia związane z Wi-Fi. Urządzenie musi obsługiwać opcję rozpoznawania nazw portów usług i adresów IP. Rozwiązanie musi mieć możliwość dodania adresów IP lub MAC hostów do czarnej listy, aby zablokować dostęp przez określony czas. Rozwiązanie powinno obsługiwać blokowanie konta po kilku niepowodzeniach logowania. Rozwiązanie musi obsługiwać konfigurację zadań przechwytywania pakietów z wieloma warunkami przechwytywania pakietów w tym samym czasie oraz ich export. Rozwiązanie musi obsługiwać standardowy SYSLOG i logowanie w formacie binarnym; rozproszone binarne przechowywanie logów na wielu serwerach logów Rozwiązanie powinno obsługiwać logowanie w pamięci lokalnej i/lub serwerach

		<p>syslog.</p> <ul style="list-style-type: none"> Rozwiązanie musi obsługiwać rejestrowanie zmiany w politykach. Rozwiązanie musi obsługiwać logowanie zaufane przy użyciu opcji TCP (RFC 3195). Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. Rozwiązanie musi obsługiwać zaplanowany raport. Raport można wyeksportować w formacie PDF/HTML/WORD za pośrednictwem email lub FTP. Rozwiązanie musi umożliwić podgląd raportów w formacie HTML i PDF. Rozwiązanie musi wspierać IPv6 dla serwera NTP. Rozwiązanie musi obsługiwać funkcję naprawy bazy danych.
17.	Polityki bezpieczeństwa	<ul style="list-style-type: none"> Proponowane rozwiązanie musi obsługiwać kontrolę dostępu do strefy (zone), użytkownika, usługi, aplikacji, IPS, AV w jednej regule polityki. Proponowane rozwiązanie musi obsługiwać wstępnie zdefiniowane i niestandardowe obiekty. Proponowane rozwiązanie musi obsługiwać weryfikację nadmiarowości polityki bezpieczeństwa oraz zliczanie trafień polityki przez interfejs WebUI. Rozwiązanie musi obsługiwać import i eksport polityk.
18.	Inteligentne funkcje bezpieczeństwa	<ul style="list-style-type: none"> Rozwiązanie musi obsługiwać analizę korelacji zagrożeń, korelację między nieznanymi zagrożeniami, nietypowe zachowanie i zachowanie aplikacji, aby wykryć potencjalne zagrożenia lub ataki. Rozwiązanie musi obsługiwać wielowymiarowe reguły analizy korelacji zagrożeń z automatyczną codzienną aktualizacją z chmury. Rozwiązanie musi obsługiwać zaawansowane wykrywanie złośliwego oprogramowania oparte na analizie zachowaniu bez sygnatur. Rozwiązanie powinno umożliwić wykrycie min. 2000 rodzin znanych i nieznanych szkodliwych programów, w tym wirusów, robaków, trojanów, itp. Rozwiązanie musi obsługiwać modelowanie zachowania w oparciu o ruch bazowy L3-L7, aby ujawnić nietypowe zachowanie sieci, takie jak skanowanie HTTP, Spider, SPAM, SSH/FTP. Rozwiązanie musi obsługiwać wykrywanie DDoS, w tym Flood, Sockstress, zip of death, mirroring, zapytanie DNS, SSL DDos i DDoS aplikacyjny na podstawie analizy nieprawidłowego zachowania. Rozwiązanie musi obsługiwać inspekcję zaszyfrowanego ruchu tunelowego dla nieznanymi aplikacji. Rozwiązanie musi obsługiwać aktualizację bazy danych modelu nieprawidłowego zachowania online i w czasie rzeczywistym. Rozwiązanie musi zapewniać widoczność zagrożeń, w tym indeks ryzyka sieciowego, krytyczne zasoby i stan ryzyka hosta, wagę i pewność ryzyka hosta i zagrożeń. Rozwiązanie musi zapewniać mapowanie Kill Chain zagrożeń na każdym hoście. Rozwiązanie powinno zapewniać analizę forensic, w tym analizę zagrożeń, bazę wiedzy, historię i PCAP. Rozwiązanie musi obsługiwać niestandardowe i wstępnie zdefiniowane reguły mitygacji zagrożeń Rozwiązanie musi obsługiwać narzędzie do przechwytywania pakietów sieciowych, które może być używane do przechwytywania pakietów na podstawie adresu źródłowego, adresu docelowego, aplikacji, protokołu, portu źródłowego, portu docelowego, rozmiaru pliku itp. Rozwiązanie musi obsługiwać przechwytywanie pakietów dla globalnej bazy sygnatur IPS lub określonych protokołów.

19.	Monitoring	<ul style="list-style-type: none"> Rozwiązanie musi posiadać pełne monitorowanie zagrożeń, w tym podawać minimum następujące informacje o ataku: nazwę ataku (typ), priorytet (ważność), czas, adres, protokół, propozycję rozwiązania problemu. Rozwiązanie musi obsługiwać usługę Threat Intelligence. Rozwiązanie musi obsługiwać statystyki i analizy ruchu w czasie rzeczywistym. Rozwiązanie powinno min. obsługiwać: monitorowanie stanu procesora, pamięci, temperatury, wentylatora, modułów zasilania.
20.	Wymiary	Max. 2U – 19 cali.
21.	Temperatura pracy	W zakresie min. 0 do 40 ⁰ C.
22.	Waga	Max. do 7 kg.
23.	Pobór prądu	Max. do 65W.
24.	Zestaw montażowy	Odpowiedni dla standardowej uniwersalnej szafy 19 cali.
25.	Instalacja/Konfiguracja	<ul style="list-style-type: none"> Wykonawca musi skonfigurować urządzenie w oparciu o wytyczne od Zmawiającego, min. w zakresie pozwalającym na prawidłowe działanie wszystkich modułów w sieci Zamawiającego, tzw. konfiguracja startowa. Wymagane jest, by wdrożenie dostarczonego rozwiązania przeprowadzi certyfikowany inżynier producenta lub dystrybutora oferowanego rozwiązania.
26.	Gwarancja/dostawa	<ul style="list-style-type: none"> Min. 12 miesięcy gwarancji uprawniającej do zgłaszania usterek sprzętowych i oprogramowania, świadczona w reżimie 8x5xNBD, umożliwiającą pobieranie nowych wersji oprogramowania i narzędzi zarządzających. Dostęp do pomocy technicznej oraz bazy wiedzy w języku polskim; baza wiedzy powinna zawierać zbiór wszystkich poradników jak konfigurować i zarządzać oferowanym urządzeniem. W ramach dostawy wymagane jest przeprowadzenie dla max. 5 osób szkolenie z obsługi i konfiguracji dostarczonego rozwiązania przez certyfikowanego inżyniera producenta lub dystrybutora oferowanego rozwiązania.