

Załącznik nr 1 do Zapytania ofertowego

Szczegółowy Opis Przedmiotu Zamówienia

1. Tablet 10,4”- 1 szt.

Lp.	Nazwa Komponentu/ parametr	Wymagane minimalne parametry techniczne
1.	Przekątna ekranu	Min 10,4"
2.	Rozdzielczość	Min 2000 x 1200
3.	Pozostałe parametry wyświetlacza	Technologia wyświetlacza: TFT Głębokość kolorów wyświetlacza: 16M
4.	System operacyjny	Android
5.	Procesor	Octa Core
6.	Taktowanie procesora	Min 1.8 GHz
7.	Taktowanie (Boost)	Min 2 GHz
8.	Zainstalowana pamięć RAM	Min 3 GB
9.	Pamięć wewnętrzna	Min 32 GB
10.	Czytnik kart pamięci	Tak
11.	Typ kart pamięci	microSD
12.	Aparat fotograficzny	Tak
13.	Aparat - Przód	Min 5 Mpix
14.	Aparat - Tył	Min 8 Mpix
15.	Szczegółowe dane aparatu	Rozdzielczość nagrywania wideo: FHD (1920 x 1080), 30 klatek/sekundę Auto Focus
16.	Komunikacja	Bluetooth 5.0 LTE (4G)
17.	Modem WWAN (3G) / LTE (4G) / 5G	Wbudowany
18.	Funkcja telefonu komórkowego	Tak
19.	GPS	Tak
20.	Gniazda we/wy	1 x 3,5 mm minijack 1 x USB 2.0
21.	Pojemność baterii	7040 mAh
22.	Typ ogniwa	Li-ion (bateria wewnętrzna)
23.	Akcesoria w zestawie	Standardowa ładowarka Kabel USB Instrukcja Kluczyk SIM/microSD
24.	Kolor	Szary
25.	Wysokość	157.4 mm
26.	Szerokość	247.6 mm
27.	Głębokość	7 mm
28.	Waga	Min 477 g
29.	Gwarancja	2 lata

2. Zestaw komputerowy z monitorem i oprogramowaniem biurowym – 5 szt.

Lp.	Nazwa Komponentu/ parametr	Wymagane minimalne parametry techniczne
1.	Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta
2.	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz

		poczty elektronicznej
3.	Procesor	Min. 6-rdzeniowy, min 3.0GHz, osiągający w zaoferowanej konfiguracji w teście PassMark CPU Mark wynik min. 19 900 punktów.
4.	Pamięć operacyjna	2 x 8GB 3200 MHz możliwość rozbudowy do 64GB
5.	Parametry pamięci masowej	Min. 512 GB SSD M.2 NVMe dla systemu operacyjnego (możliwość montażu dysku SATA III 7200 obr./min)
6.	Grafika	Zintegrowana z płytą główną, ze wsparciem dla DirectX 12.1, OpenGL 4.6, Open CL 3.0 oraz dla rozdzielczości 3840x2160@60Hz osiągająca w teście Average G3D Mark wynik na poziomie 1790 punktów (wynik zaproponowanej grafiki musi znajdować się na stronie http://www.videocardbenchmark.net)
7.	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną; wbudowany głośnik 2W
8.	Obudowa	<p>Obudowa fabrycznie konwertowalna typu MT z możliwością pracy w pozycji pionowej i poziomej, o maksymalnej sumie wymiarów 80cm posiadająca min.: 1 zewnętrzną półkę 5,25" dla napędu optycznego typu SLIM oraz min 2 wewnętrzne półki: 2 szt 3,5" dla dysku twardego. Zaprojektowana i wykonana przez producenta komputera opatrzona trwałym logo producenta, metalowa. Obudowa musi umożliwiać serwisowanie komputera bez użycia narzędzi oraz dawać możliwość instalacji drugiego dysku twardego. Otwarcie obudowy zabezpieczone śrubą serwisową, którą można odkręcić bez użycia narzędzi.</p> <p>Z przodu obudowy wymagany jest wbudowany fabrycznie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, który musi sygnalizować co najmniej:</p> <ul style="list-style-type: none"> - awarie procesora lub pamięci podręcznej procesora; - uszkodzenie lub brak pamięci RAM; - uszkodzenie płyty głównej; - uszkodzenie zasilacza; - uszkodzenie kontrolera Video. <p>Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady typu Kensington) oraz kłódki (oczko na kłódkę) a także być wyposażona w śrubę serwisową</p> <p>Zasilacz o mocy 260 W i sprawności min 93% przy 50% obciążeniu zasilacza (80 Plus PLATINIUM).</p>
9.	Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z systemem operacyjnym Windows 11 lub Windows 10.
10.	BIOS	<p>Możliwość odczytania z BIOS:</p> <ol style="list-style-type: none"> 1. Wersji BIOS 2. Modelu procesora, prędkości procesora, ilość rdzeni 3. Informacji o ilości pamięci RAM wraz z informacją o jej prędkości a także o pojemności i obsadzeniu na poszczególnych slotach 4. Informacji o dysku twardym: model, pojemność 5. Informacji o napędzie optycznym: model 6. Informacji o MAC adresie karty sieciowej <p>Możliwość wyłączenia/włączenia: zintegrowanej karty sieciowej, kontrolera audio, poszczególnych portów USB, poszczególnych slotów SATA, wewnętrznego głośnika, z poziomu BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych.</p> <p>Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.</p> <p>Możliwość - bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - ustawienia hasła na poziomie administratora.</p> <p>BIOS musi posiadać funkcję update BIOS przez sieć włączaną na poziomie BIOS przez użytkownika bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.</p>
11.	Bezpieczeństwo	<p>1. BIOS musi posiadać możliwość</p> <ul style="list-style-type: none"> - skonfigurowania hasła „Power On” oraz ustawienia hasła dostępu do BIOSu (administratora) w sposób gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS,

		<ul style="list-style-type: none"> - możliwość ustawienia hasła na dysku (drive lock) - blokady/wyłączenia portów USB, COM, karty sieciowej, karty audio; - blokady/wyłączenia poszczególnych kart rozszerzeń/slotów PCIe - kontroli sekwencji boot-ącej; - startu systemu z urządzenia USB - funkcja blokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń <p>2. Komputer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (TPM v2.0);</p> <p>3. Możliwość zapięcia linki typu Kensington i kłódki do dedykowanego oczka w obudowie komputera</p> <p>4. Udostępnione bez dodatkowych opłat oprogramowanie szyfrujące zawartość twardego dysku zgodnie z certyfikatem X.509 oraz algorytmem szyfrującym AES 256bit, współpracujące z wbudowaną sprzętową platformą bezpieczeństwa oraz zaimplementowane bezpośrednio na poziomie BIOS.</p> <p>5. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika w języku polskim, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Minimalne funkcjonalności systemu diagnostycznego:</p> <ul style="list-style-type: none"> - informacje o systemie, min.: <ol style="list-style-type: none"> 1. Procesor: typ procesora, jego obecna prędkość 2. Pamięć RAM: rozmiar pamięci RAM, osadzenie na poszczególnych slotach, szybkość pamięci, nr seryjny, typ pamięci, nr części, nazwa producenta 3. Dysk twardego: model, wersja firmware, nr seryjny, procentowe zużycie dysku 4. Napęd optyczny: model, wersja firmware, nr seryjny 5. Data wydania i wersja BIOS 6. Nr seryjny komputera: - możliwość przeprowadzenia szybkiego oraz szczegółowego testu kontrolującego komponenty komputera - możliwość przeprowadzenia testów poszczególnych komponentów a w szczególności: procesora, pamięci RAM, dysku twardego, karty dźwiękowej, klawiatury, myszy, sieci, napędu optycznego, płyty głównej, portów USB, karty graficznej - rejestr przeprowadzonych testów zawierający min.: datę testu, wynik, identyfikator awarii.
12.	Zarządzanie	Wbudowana w płytę główną technologia umożliwiająca zdalną aktualizację ustawień BIOS, bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych.
13.	Certyfikaty i standardy	<ul style="list-style-type: none"> - Certyfikat ISO 9001, ISO 14001 dla producenta sprzętu . - Deklaracja zgodności CE. - Komputer musi spełniać wymogi normy Energy Star 8.0. Wymagany certyfikat lub wpis dotyczący oferowanego modelu komputera w internetowym katalogu http://www.eu-energystar.org lub http://www.energystar.gov - - Komputer musi spełniać wymogi normy EPEAT na poziomie min Gold dla Polski. Wymagany certyfikat lub wpis dotyczący oferowanego modelu komputera w internetowym katalogu http://www.epeat.net - Komputer musi spełniać wymogi TCO Certified Desktops 8. Wymagany certyfikat lub wpis dotyczący oferowanego modelu komputera w internetowym katalogu https://tcocertified.com/
14.	Ergonomia	Maksymalnie 21 dB z pozycji operatora w trybie IDLE, pomiar zgodny z normą ISO 9296 / ISO 7779; wymaga się dostarczenia odpowiedniego certyfikatu lub deklaracji producenta.
15.	Warunki gwarancji	3-letnia gwarancja producenta świadczona na miejscu u klienta Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta.
16.	Wsparcie techniczne producenta	Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera, dostępna w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia: - weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa - CPU, HDD, pamięć)

		<p>- czasu obowiązywania i typ udzielonej gwarancji</p> <p>Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera</p> <p>Możliwość weryfikacji czasu obowiązywania i reżimu gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera</p>
17.	Wymagania dodatkowe	<ol style="list-style-type: none"> Zainstalowany system operacyjny Windows 11 Professional 64bit PL samoczynnie aktywujący się kluczem zaszytym w BIOS po podłączeniu do internetu lub system równoważny – przez równoważność rozumie się pełną funkcjonalność jaką oferuje wymagany w SIWZ system operacyjny Wbudowane porty i złącza: <ul style="list-style-type: none"> - porty video: min. 1 szt Display Port 1.4, 1 szt HDMI - min. 9 x USB wyprowadzonych na zewnątrz obudowy: <ul style="list-style-type: none"> 3 porty USB typ-A z przodu w tym: <ul style="list-style-type: none"> - min. 3 szt USB 10 Gb, 1 port USB typ-C 10 Gb z przodu, 5 portów USB typ-A z tyłu w tym min 3 szt USB 5 Gb, - port sieciowy RJ-45, - porty audio: <ul style="list-style-type: none"> audio-out z tyłu obudowy, port COMBO audio z przodu obudowy. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. Karta sieciowa 10/100/1000 Ethernet RJ 45 (zintegrowana) z obsługą PXE, WoL, ACPI Płyta główna z chipsetem min Q670, wyposażona w: <ul style="list-style-type: none"> - 2 złącza DIMM z obsługą do 64GB pamięci RAM 3200MHz DDR4 - sloty: 1 szt PCIe x16 Gen 4.0, 1 szt PCIe x1 gen 4, 1 szt PCI - 3 złącza SATA w tym min 2 szt SATA III - 2 złącza M.2 – 1 szt dedykowana dla modułu WiFi i 1 szt dedykowana dla dysków M.2 SSD Klawiatura USB w układzie polski programisty Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll) Nagrywarka SATA DVD +/-RW SLIM Czytnik kart SD 4.0 ze wsparciem dla kart SD, SDXC, SDHC, UHS-I, UHS-II <p>Karta Wi-Fi AX cat. 6 z dwoma antenami i z Bluetooth 5.2</p>
18.	Oprogramowanie biurowe	Microsoft Office Home & Business 2021 PL P8 Win/Mac Medialess Box lub równoważne
Monitor		
19.	Proporcje obrazu	16:9
20.	Przekątna ekranu	Min 23.8"
21.	Typ matrycy	VA
22.	Powierzchnia matrycy	Matowa
23.	Ekran dotykowy	Nie
24.	Technologia podświetlania	Diody LED
25.	Plamka matrycy	Max 0.2745 mm
26.	Rozdzielczość	1920 x 1080 (FHD 1080)
27.	Czas reakcji	Max 4 ms
28.	Jasność	300 nits
29.	Kontrast statyczny	3 000:1
30.	Kontrast dynamiczny	50 000 000:1
31.	Częstotliwość odświeżania	75 Hz
32.	Kąt widzenia poziomy	178 °
33.	Kąt widzenia pionowy	178 °
34.	Ilość kolorów	16,7 mln
35.	Gniazda we/wy	<ul style="list-style-type: none"> 1 x 3,5 mm minijack 1 x 15-pin D-Sub 1 x DVI 1 x HDMI

		1 x DisplayPort 4 x USB 3.0
36.	Wbudowane głośniki	2 W x 2
37.	Pivot	Tak
38.	Standard VESA	100 x 100
39.	Pobór mocy	Max 20 W
40.	Klasa energetyczna	E
41.	Akcesoria w zestawie	Kabel HDMI 1.8m Kabel zasilający
42.	Kolor	Czarny
43.	Wysokość	max 326.4 mm
44.	Wysokość z podstawą	Max 384.4 mm
45.	Szerokość	Max 540.2 mm
46.	Głębokość	Max 50.7 mm
47.	Głębokość z podstawą	Max 200.1 mm
48.	Waga	Max 4.75 kg
49.	Pozostałe parametry	Pochylenie: -5~35° Regulacja wysokości: 150mm Obrót: 180 stopni
50.	TCO Certified	Tak
51.	Informacje o gwarancji	3 lata

3. Urządzenie wielofunkcyjne laser A4 mono – 1 szt.

Lp.	Nazwa Komponentu/ parametr	Wymagane minimalne parametry techniczne
1.	Obszar zastosowań	Wydruki w biurze
2.	Typ	Urządzenie wielofunkcyjne mono A4
3.	Funkcje	Drukowanie, Kopiowanie, Skanowanie
4.	Rodzaj wydruku	Laserowy monochromatyczny
5.	Wyświetlacz	kolorowy dotykowy, graficzny ekran LCD 4,3''
6.	Standardowa szybkość drukowania A4	Co najmniej 46 str./min.
7.	Wydruk pierwszej strony	Do 8 sek.
8.	Czas nagrzewania	Mniej niż 4,7 sekundy z trybu uśpienia
9.	Interfejsy połączeniowe	10/100/1000 BaseT Ethernet, Hi-Speed USB 2.0, sieć bezprzewodowa (IEEE 802.11b/g/n), AirPrint
10.	Druk obustronny	automatyczny
11.	Główny podajnik papieru	Min 500 arkuszy 75g/m ²
12.	Podajnik ADF	80 arkuszy (papier zwykły 75 g/m ²)
13.	Maksymalna pojemność podajników	2500 arkuszy 75 g/m ²
14.	Rozdzielczość drukowania	Co najmniej 1200 x 1200 dpi
15.	Zainstalowanej pamięci RAM	Co najmniej 512 MB
16.	Procesor- taktowanie	Co najmniej 800MHz
17.	Szybkość kopiowania mono	Do 46 kopii na minutę
18.	Kopiowanie dwustronne	Automatyczne
19.	Możliwość skanowania	Mono i kolor
20.	Skanowanie do	Bezpośrednie skanowanie do pamięci Flash USB. Obsługiwane formaty plików: PDF, PDF/A,

		zabezpieczony PDF, podpisany PDF, JPEG, XPS, TIFF
21.	Skanowanie dwustronne	Automatyczne
22.	Szybkość skanowania dwustronnego A4	50 str./min w czerni w rozdzielczości 300 dpi
23.	Prędkość skanowania	Do 100 obrazów na minutę
24.	Możliwość skanowania ręcznego	Tak
25.	Rekomendowana przez producenta eksploatacja w zestawie	pozwalająca wydrukować 7 500 stron zgodnie z normą ISO/IEC 19752
26.	Czytnik NFC	wbudowany
27.	Toner superwydajny	Opcjonalny do 12 000 stron zgodnie z normą ISO/IEC 19752- nie jest wymagane dostarczenie
28.	Obciążenie miesięczna	Do 125 000 stron
29.	Sterowniki	Windows 8/10/ (32/64-bit)
30.	CE	Urządzenie posiada oznakowanie CE.
31.	Zasilanie	230V~50 Hz
32.	Inne wymagania	Sprzęt musi być fabrycznie nowy
33.	Gwarancja	Producenta- min. 36 miesięcy w miejscu instalacji

4. Laptop 17,3” z oprogramowaniem biurowym - 3 szt.

Lp.	Nazwa Komponentu/parametr	Wymagane minimalne parametry techniczne monitoru
1.	Typ	Komputer przenośny typu notebook z ekranem 17,3” o rozdzielczości: FHD (1920x1080) UWVA IPS Non-Touch w technologii LED przeciwoodblaskowy, jasność min 300 nitów, kontrast 1000:1
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.	Procesor	Procesor klasy x86, łączna ilość rdzeni minimum 10, zaprojektowany do pracy w komputerach przenośnych, z pamięcią last level cache CPU co najmniej 12 MB lub równoważny 10 rdzeniowy procesor klasy x86 Zaferowany procesor musi uzyskiwać jednocześnie w teście Passmark CPU Mark wynik min.: 13 500 punktów (wynik zaproponowanego procesora musi znajdować się na stronie http://www.cpubenchmark.net) W przypadku użycia przez oferenta testów wydajności Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego.
4.	Pamięć operacyjna RAM	16GB 3200 MHz DDR4, możliwość rozbudowy do min 32GB
5.	Parametry pamięci masowej	Min. 512 GB SSD M.2, możliwość instalacji dodatkowego dysku 2,5” 1TB 5400rpm SATA
6.	Karta graficzna	Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej, ze sprzętowym wsparciem dla DirectX 12 osiągająca w teście Average G3D Mark wynik na poziomie min.: 2600 punktów (wynik zaproponowanej grafiki musi znajdować się na stronie

		http://www.videocardbenchmark.net
7.	Wyposażenie multimedialne	Karta dźwiękowa stereo, wbudowane dwa głośniki stereo Wbudowana w obudowę matrycy kamera HD wraz z mikrofonem
8.	Wymagania dotyczące baterii i zasilania	3-cell, 41Whr, Li-Ion, Long-Life. Zasilacz o mocy min. 45W Czas pracy na baterii wg dokumentacji producenta min 7 godzin
9.	System operacyjny	Zainstalowany 64-bitowy system operacyjny Microsoft Windows 11 Professional PL
10.	Certyfikaty i standardy	<ul style="list-style-type: none"> - Certyfikat ISO9001:2000 dla producenta sprzętu - Certyfikat ISO 14001 dla producenta sprzętu - Deklaracja zgodności CE - Spełnienie kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki - komputer musi znajdować się na liście zgodności WHCL Microsoft potwierdzającej zgodność oferowanego komputera z oferowanym system operacyjnym - Certyfikat EPEAT 2019 na poziomie GOLD dla Polski Certyfikat EnergyStar v 8.0 – komputer musi znajdować się na liście zgodności dostępnej na stronie www.energystar.gov
11.	Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie (IDLE) wynosząca maksymalnie 21.8dB (wartość do zweryfikowania w dokumentacji technicznej komputera).
12.	Waga i wymiary	Waga max 2.10 kg z baterią 3-cell Szerokość: max 401 mm Głębokość: max 258 mm Wysokość: max 19,9 mm
13.	BIOS	Możliwość odczytania z BIOS: 1. Wersji BIOS wraz z datą wydania wersji 2. Modelu procesora, prędkości procesora, wielkość pamięci cache L1/L2/L3 3. Informacji o ilości pamięci RAM wraz z informacją o jej prędkości, pojemności, producencie i obsadzeniu na poszczególnych slotach 4. Informacji o dysku twardym: typ, producent, model Możliwość wyłączenia/włączenia: kontrolera audio, portów USB, wewnętrznych głośników, mikrofonu, karty dźwiękowej, wirtualizacji, bluetooth, modułu WiFi z poziomu BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Możliwość bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - ustawienia hasła na poziomie administratora.
14.	Bezpieczeństwo	TPM 2.0 1. BIOS musi posiadać możliwość <ul style="list-style-type: none"> - skonfigurowania hasła „Power On” oraz ustawienia hasła dostępu do BIOSu (administratora) w sposób gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS, - blokady/wyłączenia portów USB, karty audio; - blokady/wyłączenia poszczególnych kart rozszerzeń - kontroli sekwencji boot-ujące; - startu systemu z urządzenia USB

		<p>- funkcja blokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń</p> <p>2. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika w języku polskim, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Minimalne funkcjonalności systemu diagnostycznego:</p> <p>- informacje o systemie, min.:</p> <ol style="list-style-type: none"> 1. Procesor: typ procesora, jego obecna prędkość 2. Pamięć RAM: rozmiar pamięci RAM, osadzenie na poszczególnych slotach, szybkość pamięci, nr seryjny, typ pamięci, nr części, nazwa producenta 3. Dysk twardy: model, wersja firmware, nr seryjny, procentowe zużycie dysku 4. Bateria: nr seryjny, napięcie 5. Data wydania i wersja BIOS 6. Nr seryjny komputera <p>- możliwość przeprowadzenia szybkiego oraz szczegółowego testu kontrolującego komponenty komputera</p> <p>- możliwość przeprowadzenia testów poszczególnych komponentów a w szczególności: procesora, pamięci RAM, dysku twardego, karty dźwiękowej, klawiatury, myszy, sieci, płyty głównej, kamery internetowej, modułu wifi, portów USB, karty graficznej, baterii</p> <p>- rejestr przeprowadzonych testów zawierający min.: datę testu, wynik, identyfikator awarii</p>
15.	Warunki gwarancji	<p>36 miesięcy gwarancji producenta NBD świadczona na miejscu u klienta</p> <p>Czas reakcji serwisu - do końca następnego dnia roboczego</p> <p>Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta komputera</p> <p>Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego.</p>
16.	Wymagania dodatkowe	<ol style="list-style-type: none"> 1. Wbudowane porty i złącza: 1 x HDMI 1.4, 2 szt. USB 3.2 Gen 1, 1 szt USB typ-C 3.2. Gen 1, 1 x złącze słuchawkowe stereo/liniowe wyjście + złącze mikrofonowe (COMBO audio), wbudowana kamera HD w obudowę ekranu komputera + mikrofon. 2. Karta WLAN 802.11 ac 2x2 wraz z Bluetooth 5.0 COMBO, zintegrowany z płytą główną lub w postaci wewnętrznego modułu. 3. Klawiatura (układ US -QWERTY) z wydzieloną z prawej strony klawiaturą numeryczną 4. Clickpad. 5. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. <p>Zewnętrzna karta sieciowa USB- LAN 1 x 10/100/1000 Mbit/s</p>
17.	Oprogramowanie biurowe	<p>Oprogramowanie biurowe Microsoft Office Home & Business 2021 PL P8</p> <p>Win/Mac Medialess – lub równoważne</p>

5. Monitor 27” – 2 szt.

Lp.	Nazwa Komponentu/ parametr	Wymagane minimalne parametry techniczne
1.	Proporcje obrazu	16:9
2.	Przekątna ekranu	Min 23.8"
3.	Typ matrycy	VA
4.	Powierzchnia matrycy	Matowa

5.	Ekran dotykowy	Nie
6.	Technologia podświetlania	Diody LED
7.	Plamka matrycy	Max 0.2745 mm
8.	Rozdzielczość	1920 x 1080 (FHD 1080)
9.	Czas reakcji	Max 4 ms
10.	Jasność	300 nits
11.	Kontrast statyczny	3 000:1
12.	Kontrast dynamiczny	50 000 000:1
13.	Częstotliwość odświeżania	75 Hz
14.	Kąt widzenia poziomy	178 °
15.	Kąt widzenia pionowy	178 °
16.	Ilość kolorów	16,7 mln
17.	Gniazda we/wy	<ul style="list-style-type: none"> • 1 x 3,5 mm minijack • 1 x 15-pin D-Sub • 1 x DVI • 1 x HDMI • 1 x DisplayPort • 4 x USB 3.0
18.	Wbudowane głośniki	2 W x 2
19.	Pivot	Tak
20.	Standard VESA	100 x 100
21.	Pobór mocy	Max 20 W
22.	Klasa energetyczna	E
23.	Akcesoria w zestawie	<ul style="list-style-type: none"> • Kabel HDMI 1.8m • Kabel zasilający
24.	Kolor	Czarny
25.	Wysokość	Max 326.4 mm
26.	Wysokość z podstawą	Max 384.4 mm
27.	Szerokość	Max 540.2 mm
28.	Głębokość	Max 50.7 mm
29.	Głębokość z podstawą	Max 200.1 mm
30.	Waga	Max 4.75 kg
31.	Pozostałe parametry	<ul style="list-style-type: none"> • Pochylenie: -5~35° • Regulacja wysokości: 150mm • Obrót: 180 stopni
32.	TCO Certified	Tak
33.	Informacje o gwarancji	3 lata

6. Urządzenie typu UTM ze szkoleniem informatyka z obsługi urządzenia - 1 szt.

Lp.	Nazwa Komponentu/ parametr	Wymagane minimalne parametry techniczne
1.	Wymagania Ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych

		<p>aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> - Firewall. - Ochrony w warstwie aplikacji. - Protokołów routingu dynamicznego.
2.	Redundancja, monitoring i wykrywanie awarii	<p>W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastr Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.</p> <p>Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.</p> <p>Monitoring stanu realizowanych połączeń VPN.</p> <p>System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.</p>
3.	Interfejsy, Dysk, Zasilanie:	<p>System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:</p> <ul style="list-style-type: none"> 10 portami Gigabit Ethernet RJ-45. <p>System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</p> <p>System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.</p> <p>System jest wyposażony w zasilanie AC.</p>
4.	Parametry wydajnościowe:	<p>W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.</p> <p>Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.</p> <p>Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.</p> <p>Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.</p> <p>Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.</p> <p>Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 750 Mbps.</p> <p>Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 650 Mbps.</p>
5.	Funkcje Systemu Bezpieczeństwa:	<p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ul style="list-style-type: none"> Kontrola dostępu - zaporą ogniową klasy Stateful Inspection. Kontrola Aplikacji. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. Ochrona przed malware. Ochrona przed atakami - Intrusion Prevention System. Kontrola stron WWW. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. Zarządzanie pasmem (QoS, Traffic shaping).

		<p>Mechanizmy ochrony przed wyciekami poufnej informacji (DLP).</p> <p>Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.</p> <p>Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.</p> <p>Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.</p> <p>Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).</p>
6.	Polityki, Firewall	<p>Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</p> <p>System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:</p> <p>Translację jeden do jeden oraz jeden do wielu.</p> <p>Dedykowany ALG (Application Level Gateway) dla protokołu SIP.</p> <p>W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</p> <p>Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.</p> <p>Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</p> <p>Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</p> <p>Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.</p> <p>Amazon Web Services (AWS).</p> <p>Microsoft Azure.</p> <p>Cisco ACI.</p> <p>Google Cloud Platform (GCP).</p> <p>OpenStack.</p> <p>VMware NSX.</p> <p>Kubernetes.</p>
7.	Połączenia VPN	<p>System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:</p> <p>Wsparcie dla IKE v1 oraz v2.</p> <p>Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).</p> <p>Obsługa protokołu Diffie-Hellman grup 19, 20.</p> <p>Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.</p> <p>Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.</p> <p>Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</p> <p>Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.</p> <p>Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.</p>

		<p>Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.</p> <p>Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.</p> <p>Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.</p> <p>Mechanizm „Split tunneling” dla połączeń Client-to-Site.</p> <p>System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:</p> <p>Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.</p> <p>Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.</p> <p>Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.</p>
8.	Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie zapewnia obsługę:</p> <p>Routingu statycznego.</p> <p>Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).</p> <p>Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.</p> <p>Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.</p> <p>ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.</p> <p>BFD (Bidirectional Forwarding Detection).</p> <p>Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.</p>
9.	Funkcje SD-WAN	<p>System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.</p> <p>SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</p>
10.	Zarządzanie pasmem	<p>System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</p> <p>System daje możliwość określania pasma dla poszczególnych aplikacji.</p> <p>System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</p> <p>System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.</p>
11.	Ochrona przed malware	<p>Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</p> <p>System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.</p>

		<p>System umożliwi blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</p> <p>System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</p> <p>Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.</p> <p>System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.</p> <p>Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratorium producenta.</p> <p>Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</p>
12.	Ochrona przed atakami	<p>Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>System chroni przed atakami na aplikacje pracujące na niestandardowych portach.</p> <p>Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p> <p>Mechanizmy ochrony dla aplikacji Web`owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</p> <p>Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.</p> <p>Wykrywanie i blokowanie komunikacji C&C do sieci botnet.</p> <p>Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.</p>
13.	Kontrola aplikacji	<p>Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</p> <p>Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</p> <p>Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).</p>
14.	Kontrola WWW	<p>Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</p>

		<p>W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</p> <p>Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.</p> <p>Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</p> <p>Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</p> <p>Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</p> <p>Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</p> <p>System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.</p>
15.	Uwierzytelnianie użytkowników w ramach sesji	<p>System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</p> <p>Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</p> <p>Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</p> <p>System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.</p> <p>System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.</p> <p>Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</p>
16.	Zarządzanie	<p>Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.</p> <p>Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>Istnieje możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.</p> <p>System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</p> <p>System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p> <p>Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</p>

		Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
17.	Logowanie	<p>Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.</p> <p>W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p> <p>Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</p> <p>Możliwość włączenia logowania per reguła w polityce firewall.</p> <p>System zapewnia możliwość logowania do serwera SYSLOG.</p> <p>Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p>
18.	Certyfikaty	Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall.
19.	Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
20.	Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.
21.	Gwarancja oraz wsparcie	Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
22.	Opisy do wymagań ogólnych	Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

7. Zasilanie UPS z agregatem i rozdzielnicą

Zamawiający wymaga dostarczenia:

- agregat prądowórczego w obudowie zewnętrznej dźwiękoszczelnej o mocy co najmniej **18kVA/14,4kW- 1 szt.**
- zasilaczy UPS 2,2kVA/1,98kW- 2 szt.

Zasilacze UPS (2 szt.) mają za zadanie podtrzymanie zasilania urządzeń zamontowanych w szafach rackowych serwerowni w piwnicy. Agregat prądowórczy ma za zadanie utrzymanie zasilania tylko w pomieszczeniach w piwnicy związanych z samą serwerownią jak i pomieszczeniami pomocniczymi. Agregat zasilony rozdzielnicą R0 w piwnicy

Montaż agregatu prądowórczego przewiduje się na parkingu, przy ścianie zewnętrznej serwerowni (ściana szczytowa nowej części budynku). Na potrzeby agregatu należy wykonać **sztuczny uziom**, zamontować w wejściu głównym do obiektu **wyłącznik p.pożarowy** oraz wyprowadzić z rozdzielnicy R0 **obwód(y) potrzeb własnych agregatu**.

W klatce schodowej w piwnicy obok istniejącej rozdzielnicy R0 należy zainstalować układ SZR, którego zadaniem będzie śledzenie parametrów sieci zasilającej i w razie stanów awaryjnych uruchamianie agregatu prądowórczego i przełączanie na niego odbiorów. Wykonawca zaprojektuje i wykona montaż układu SZR przy rozdzielnicy R0.

7.1 Zasilanie UPS 2200VA – 2 sztuki

Lp.	Nazwa Komponentu/ parametr	Wymagania
1.	UPS	2200 VA / 1980 W
2.	Technologia pracy	true on-line (VFI zgodnie ze standardem IEC 62040-3)
3.	Obudowa	Możliwość konfiguracji montażowej TOWER oraz RACK
4.	Konfiguracja UPS	1/1
5.	Sprawność w trybie podwójnej konwersji ON-LINE	>92%
6.	Sprawność w trybie Economy	do 98%
7.	Smart Active	Automatyczny wybór tryb pracy on-line lub line interactive w zależności od mierzonych parametrów jakości zasilania głównego
8.	Panel wyświetlacza	Obracany panel wyświetlacza
9.	Automatyczny restart (po powrocie zasilania z sieci, po rozładowaniu baterii)	wymagane
10.	Możliwość instalacji w wersji wolnostojącej TOWER lub RACK	Wymiary TOWER. Wersja RACK wymiary odpowiednie dla montażu w szafie 19", 2U wymiary W x D x H [mm] 87 x 625 x 450
WEJŚCIE		
11.	Napięcie znamionowe	220 - 230 – 240 V
12.	Minimalne napięcie	140-276 V przy 50% obciążeniu, 184-276 V 100% obciążeniu
13.	Maksymalne napięcie pracy - wejściowe	300 V
14.	Częstotliwość znamionowa	50–60 Hz ± 5 Hz
15.	Współczynnik mocy	> 0,98
16.	Zniekształcenia prądu	≤ 7%

17.	Możliwość współpracy z generatorem prądowtórzym	wymagane
BYPASS wewnętrzny		
18.	Tolerancja napięcia	200 – 253 V (do wyboru w trybie Economy lub Smart Active)
19.	Tolerancja częstotliwości	Wybrana częstotliwość $\pm 5\%$ (ustawialny)
20.	Przeciążalność	125% przez 4s, 150% przez 0,5 s
WYJŚCIE		
21.	Napięcie znamionowe	220-230-240 V
22.	Zniekształcenie napięcia	< 2%
23.	Częstotliwość	50Hz / 60Hz lub automatycznie
24.	Statyczna stabilność napięcia	$\pm 1\%$
25.	Dynamiczna stabilność napięcia	$\leq 5\%$ w czasie 20 ms
26.	Kształt napięcia	Sinusoidalny
27.	Współczynnik szczytu	3:1
28.	Sprawność w trybie ECO i Smart Active	98%
BATERIE		
29.	Typ	Bezobsługowe, ołowiane w technologii VRLA AGM
30.	Bateria w UPS „hot-swap”	Funkcja „hot-swap” wymagane
31.	Czas ładowania	2 – 4 h
32.	Czas pracy autonomicznej	6 minut przy obciążeniu mocą 1540W
33.	Możliwość wydłużenia czasu podtrzymania przez instalację dodatkowych baterii	wymagane
INNE		
34.	Zabezpieczenia	Nadmiarowoprądowe – zwarciove – przeciwprzepięciowe – nadnapięciowe – temperaturowe – przeciw nadmiernemu wyczerpaniu baterii
35.	Komunikacja	USB/DB9 + RS232 + gniazdo na dodatkową kartę komunikacji
36.	Gniazdo wejściowe	Listwa zaciskowa 1 IEC 320 C20
37.	Gniazda wyjściowe	Listwa zaciskowa 8 IEC 320 C13 + 1 IEC 320 C19
38.	Standardy komunikacyjne	port USB / DB9 z RS232 i stykami / gniazdo na kartę komunikacyjną takie jak: Modbus/JBUS, TCP/IP-SNMP i przekaźniki
39.	Opcje interfejsów komunikacyjnych	Zaawansowana komunikacja dla systemów operacyjnych i środowisk sieciowych, POWERSHIELD3, możliwość współpracy z Windows, Hyper-V, 2012, 2008 i wcześniejszymi, Mac OS X, Linux, VMWare ESXi, Citrix XenServer oraz z innymi systemami operacyjnymi Unix.
40.	Karta do komunikacji	Karta sieciowa
41.	Inne	Zestaw szyn do montażu w szafie rack
42.	Normy	Bezpieczeństwo: EN 62040-1 oraz dyrektywa 2006/95/EL; EMC: EN 620040-2 kategoria C2 oraz dyrektywa 2004/108/EL
43.	Certyfikaty	CE
44.	Temperatura pracy	0° C / +40° C
45.	Wilgotność	<90% bez kondensacji pary wodnej
46.	Głośność Poziom hałasu z 1m w trybie ECO	< 40 dBA
47.	Dostawa i uruchomienie w	wymagane

	miejscu instalacji	
48.	Gwarancja fabryczna Producenta w miejscu instalacji Gwarancja dotyczy UPS oraz akumulatorów.	24 miesiące

7.2. Agregat 18 kVA/ 14,4 kW – 1 sztuka

Agregat prądowórczy o mocy znamionowej (PRP) 18 kVA/ 14,4 kW (zgodnie z ISO8528) i mocy awaryjnej 20kVA/ 16kW (zgodnie z ISO8528) z automatycznym panelem sterowania. Agregat umieszczony w obudowie odpornej na warunki atmosferyczne. Obudowa przystosowana do montażu zewnętrznego z redukującą poziom hałasu do 71,5 dB(A) z 7m.

Agregat prądowórczy wyposażony w:

- Silnik przemysłowy, wraz z systemem chłodzenia, wtryskiem z automatyczną kontrolą prędkości, elektrycznym zapłonem i ładowarką bateryjną,
- Silnik 4-cylindrowy, wysokoprężny, turbodiesel, chłodzony cieczą silnik typu: BAUDOIN model 4M06G20/5,
- Moc silnika w trybie PRP 18kW,
- prądnicą (przemysłowa, bezszczotkowa prądnicą z automatycznym, elektronicznym systemem kontroli nadpęcia AVR, samowzbudna), stopień ochrony IP23, klasa izolacji H, z automatycznym, elektronicznym regulatorem napięcia AVR, statyczną dokładnością regulacji napięcia 1.0 ±%,
- moc pozorna prądnicy 18,8kVA,
- agregat wyposażony w automatyczny panel sterowania ComAp AMF25 w jez. polskim, wymagania:
 - 3 konfigurowalne wejścia analogowe
 - Wejście czujnika magnetycznego
 - Zacisk wstępnego wzbudzenia D+
 - 7 wejść binarnych
 - 7 wyjść binarnych
 - Automatyczne i ręczne sterowanie GCB i MCB
 - Sieć CAN z obsługą J1939
 - Możliwość dołączenia modułów rozszerzenia wtykowych i dotyczących magistrali CAN
 - Dziennik zdarzeń i pracy RTC
 - Podwójny system AMF/z wzajemną rezerwą
 - Pomiar prądu/mocy agregatu prądowórczego
- dzienny zbiornik paliwa o pojemności 62l. umiejscowiony w ramie agregatu, umożliwiający przez 13,19 godzin pracy agregatu przy 100% obciążeniu z jednego napełnienia zbiornika (spalanie przy 100% obc. PRP 4,7 l/h),
- zbiornik z elektronicznym czujnikiem poziomu paliwa,
- pompa spuszczenia oleju silnikowego,
- elektroniczny regulator prędkości obrotowej silnika,
- elektroniczny regulator napięcia AVR,
- automatyczny układ podgrzewania płynu chłodzącego,
- amortyzatory antywibracyjne zainstalowane między ramą a układem silnik-prądnicą,
- tłumik wydechu spalin,
- wyłącznik główny z zabezpieczeniem przeciwzwarciovym i przeciążeniowym generatora 3P ABB,
- Agregat wyposażony w SZR panel przełączenia agregat / sieć,
- Maksymalne wymiary agregatu: (dł. x szer. x wys. w mm; masa netto w kg): 2000 x 1000 x 1300, waga 750kg,
- Dostawa, montaż i uruchomienie

Zamawiający przygotowuje podbudowę pod agregat we własnym zakresie w uzgodnieniu z Dostawcą. Dostawca agregatu prądowórczego zobowiązany jest o potwierdzenie spełnienia wszystkich wymaganych parametrów technicznych z załączeniem kart katalogowych. Zamawiający zastrzega sobie prawo do weryfikacji deklarowanych przez Dostawcę parametrów elektrycznych urządzenia już po zainstalowaniu. W przypadku, jeśli wyniki pomiarów, przeprowadzonych przez specjalistyczną firmę, nie potwierdzą deklarowanych parametrów, Zamawiający zastrzega sobie prawo anulowania zamówienia i obciążenia Dostawcę kosztami pomiarów.



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Instalacja elektryczna sprowadza się do wykonania połączeń pomiędzy agregatem prądotwórczym, panelem kontroli i układem SZR oraz podłączenia kabli zasilających do układu SZR.

Wszelkie prace instalacyjne, naprawy i konserwacja powinny być przeprowadzone przez w pełni wykwalifikowanych i doświadczonych instalatorów. Połączenia elektryczne powinny być wykonane zgodnie z obowiązującymi normami ze szczególnym uwzględnieniem uziemienia.

Kontrola i przygotowanie agregatu prądotwórczego do pierwszego rozruchu leżą w kompetencji służb technicznych dostawcy agregatu.

Z pierwszego uruchomienia agregatu należy sporządzić protokół.

Służby techniczne po pierwszym uruchomieniu agregatu mają też obowiązek przeprowadzić szkolenie osób wyznaczonych przez Zamawiającego do obsługi dostarczonego agregatu.