Zakup sprzętu komputerowego wraz z oprogramowaniem dla Gminy Marciszów w ramach projektu "Cyfrowa Gmina"

OPZ – Opis Przedmiotu Zamówienia

ZP/271/12/22

Załącznik nr 4

Tabela nr 1

Szczegółowy opis			**Parametry oferowane**
Komputer przenośny. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy (numer konfiguracji lub part numer) oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. Jeśli na stronie internetowej producenta nie jest dostępna pełna oferta modeli sprzętu wraz z jego konfiguracją, do oferty należy dołączyć katalog producenta zaoferowanego produktu umożliwiający weryfikację oferty pod kątem zgodności z wymaganiami Zamawiającego.			Producent: Model: Numer katalogowy (numer konfiguracji lub part numer):
Nie dopuszcza się modyfikacji na drodze Producent-Zamawiający.			
Zamawiający zastrzega sobie prawo do sprawdzenia reżimu gwarancyjnego oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu.			
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
1.	Procesor	Procesor klasy x86, min. czterordzeniowy , zaprojektowany do pracy w komputerach przenośnych. Zaoferowany procesor musi uzyskiwać w teście Passmark CPU Mark średni wynik minimum 6430 punktów na dzień 18.03.2022. Lista wyników testów w załączniku.	Podać nazwę i model procesora
2.	Pamięć operacyjna RAM	Min. 8 GB 2666MHz non-ECC Możliwość rozbudowy do 64GB pamięci operacyjnej pracującej w trybie dual channel.	spełnia / nie spełnia
3.	Parametry pamięci masowej	M.2 512 GB SSD PCIe 3.0 NVMe	spełnia / nie spełnia
4.	Karta graficzna	Zintegrowana z procesorem	spełnia / nie spełnia
5.	Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki stereo (2x2W), Port słuchawek i mikrofonu typu COMBO, kamera IR video 720p z	spełnia / nie spełnia

		mechaniczną zasłoną obiektywu, dwa mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute).	
6.	Obudowa	Wykonana z materiałów o podwyższonej odporności na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych, charakteryzujący się wzmocnioną konstrukcją, tzw. „business rugged", według normy Mil-Std-810G	spełnia / nie spełnia
		W celu potwierdzenia, że oferowana dostawa odpowiada wymaganiom określonym przez Zamawiającego, do oferty należy dołączyć oświadczenie producenta lub inny dokument pochodzący od producenta, potwierdzający, że komputer spełnia standardy MIL-STD-810G, i pozytywnie przeszedł testy w zakresie minimum wyżej wymienionych. Dopuszcza się dokument w języku angielskim.	
7.	Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej.	spełnia / nie spełnia
8.	Zgodność z systemami operacyjnymi	Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera). Dopuszcza się dokument w języku angielskim.	spełnia / nie spełnia
9.	Bezpieczeństwo	Zintegrowany z płytą główną 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 zapisanego w TPM2.0 z certyfikacją TCG. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. Wbudowane w obudowę gniazdo dla linki zabezpieczającej.	spełnia / nie spełnia
10.	System diagnostyczny	Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia błędów zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. Działający nawet w przypadku uszkodzenia dysku twardego. System umożliwiający wykonanie minimum następujących czynności diagnostycznych: wykonanie testu: pamięci ram, procesora, pamięci masowej, matrycy lcd, magistrali pci-e, płyty głównej (chipset, usb), klawiatury, myszy, akumulatora ,wentylatora. Ponadto zaimplementowany dźwiękowy system diagnostyczny producenta umożliwiający identyfikację następujących zdarzeń: • Awaria głównej magistrali systemowej • Awaria wentylatora • Awaria modułu pamięci	spełnia / nie spełnia
		• Awaria karty rozszerzeń (M.2, PCIe) • Awaria modułu TPM • Awaria dedykowanej karty graficznej (PCIe)	

		• Awaria zintegrowanej karty graficznej (w CPU) • Awaria połączenia pomiędzy jednostką, a wyświetlaczem	
11.	BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - wersji BIOS - daty produkcji BIOS - nr seryjnym komputera - Ilości zainstalowanej pamięci RAM oraz możliwość odczytania informacji o obłożeniu, szybkości i rodzaju z poziomu BIOS lub w zaimplementowanym systemie diagnostycznym – typie procesora i jego prędkości – MAC adresu zintegrowanej karty sieciowej – nr inwentarzowym (tzw. Asset Tag) - wymagane wolne pole do edycji przez administratora – nr seryjnym płyty głównej komputera – informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: – Możliwość Wyłączania/Włączania technologii antykradzieżowej - Możliwość zaawansowanego zarządzania dostępem do BIOS poprzez mechanizm wielopozowych haseł umożliwiających co najmniej: **o** Możliwość ustawienia hasła Administratora **o** Możliwość ustawienia hasła na zainstalowanym dysku SSD/HDD **o** Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password	spełnia / nie spełnia
		o Możliwość przeglądania ustawień BIOS z poziomu użytkownika bez możliwości zmiany ustawień BIOS **o** Możliwość zabezpieczenia hasłem aktualizacji BIOS – Możliwość ustawienia minimalnych wymagań dotyczących długości hasła POWER-On oraz hasła dysku twardego. – Obsługa haseł o długości min. 128 znaków zawierających: duże litery, małe litery, znaki specjalne, cyfry – Możliwość wymuszenia silnych haseł ustawianych w BIOS tzn. składających się z co najmniej ośmiu znaków z min. jedną małą literą, jedną dużą literą oraz jedną cyfrą. – Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS – Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. – Autoryzacja dostępu do aktualizacji BIOS dla użytkownika, Administratora lub z poziomu Windows – Możliwość Wyłączania/Włączania zabezpieczenia przed wgraniem starszej wersji BIOS niż aktualna – Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, karty WiFi, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, portów USB, bluetooth, czytnik kart pamięci, czytnik karta inteligentnych, zintegrowanej karty dźwiękowej, mikrofon.	

		– Możliwość włączenia/wyłączenia funkcji klonowania adresu MAC dla stacji dokującej – Możliwość niezależnego włączenia/wyłączenia płytki dotykowej oraz manipulatora (joysticka) – Funkcja bezpiecznego usuwania danych z dysku dostępna z poziomu BIOS	
12.	Ekran	Matowy, matryca TFT 15,6" z podświetleniem w technologii LED, rozdzielczość FHD 1920x1080, jasność min. 250nits, kontrast min. 700:1 w technologii IPS Kąt otwarcia pokrywy ekranu min.180 stopni.	spełnia / nie spełnia
13.	Interfejsy / Komunikacja	2xUSB 3.2 Gen. 1 typ A, 2xUSB-C 3.2 (w tym 1x Gen 2), złącze słuchawek i złącze mikrofonu typu COMBO, HDMI min. 1.4b, RJ-45. Złącze umożliwiające podpięcie linki antykradzieżowej, czytnik kart pamięci, czytnik kart smartcard. Komputer w ramach posiadanych portów musi umożliwiać dokowanie za pośrednictwem portu Thunderbolt 3 lub dedykowanego złącza umożliwiającego podłączenie mechanicznej stacji dokującej.	spełnia / nie spełnia
14.	Karta sieciowa LAN	10/100/1000 wspierająca Wake on Lan, PXE Boot,	spełnia / nie spełnia
15.	Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie AX Bluetooth min. 5.1	spełnia / nie spełnia
16.	Karta sieciowa WWAN	Możliwość instalacji (rozbudowy) modemu LTE	spełnia / nie spełnia
17.	Klawiatura	Klawiatura odporna na zalanie cieczą (funkcjonalność potwierdzona w ulotce katalogowej produktu), układ US, klawiatura wyposażona w 2 stopniowe podświetlanie przycisków.	spełnia / nie spełnia
18.	Czytnik linii papilarnych	Wbudowany czytnik linii papilarnych	spełnia / nie spełnia
19.	Napęd optyczny	Możliwość podłączenia nagrywarki DVD.	spełnia / nie spełnia
20.	Akumulator	Pozwalający na nieprzerwaną pracę urządzenia do 8 godzin - załączyć test Mobile Mark 2018 lub kartę katalogową oferowanego komputera potwierdzającą czas pracy na zasilaniu bateryjnym. Dopuszcza się dokument w języku angielskim. Ponadto komputer ma być wyposażony w system szybkiego ładowania akumulatora, który umożliwia szybkie naładowanie akumulatora notebooka do 80% w ciągu jednej godziny	spełnia / nie spełnia
21.	Zasilacz	Zasilacz zewnętrzny min. 65W	spełnia / nie spełnia
22.	Certyfikaty, oświadczenia i standardy	- Dla producenta sprzętu należy dostarczyć certyfikat: **o** ISO 9001:2015 **o** ISO 14001 **o** ISO 50001 Dopuszcza się certyfikaty w języku angielskim. - ENERGY STAR 8.0 - TCO lub TCO Edge - Deklaracja zgodności CE (załączyć do oferty). Dopuszcza się dokument w języku angielskim. - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki. Dopuszcza się dokument w języku angielskim.	spełnia / nie spełnia

		- Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy (IDLE) wynosząca maksymalnie 18 dB (załączyć oświadczenie producenta). Dopuszcza się dokument w języku angielskim.	
23.	Waga/Wymiary	Waga urządzenia z akumulatorem max. 1,98 kg Grubość notebooka nie większa niż: 21 mm	spełnia / nie spełnia
24.	System operacyjny	Zainstalowany system operacyjny umożliwiający szyfrowanie danych, pracę grupową oraz pracę w domenie; nie dopuszcza się w tym zakresie licencji oraz nośników pochodzących z rynku wtórnego. Licencja systemu operacyjnego zaimplementowana w BIOS komputera, umożliwiająca instalację systemu bez podawania klucza oraz bez aktywacji systemu za pośrednictwem Internetu. Nie dopuszcza się licencji edukacyjnej.	Podać nazwę i wersję systemu
25.	Oprogramowanie do aktualizacji sterowników	Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.	spełnia / nie spełnia Podać nazwę oprogramowania
26.	Gwarancja	Minimalny czas trwania gwarancji wynosi 2 lata.	spełnia / nie spełnia
27.	Wsparcie techniczne producenta	– Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera – Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania - możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00-18:00 Wsparcie techniczne świadczone przez producenta lub autoryzowanego partnera dla urządzeń i preinstalowanego oprogramowania OEM, zakupionego z urządzeniem, dostarczane zdalnie. Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta. Możliwość sprawdzenia konfiguracji sprzętowej komputera po podaniu numeru seryjnego bezpośrednio na stronie producenta.	spełnia / nie spełnia

Tabela nr 2

Szczegółowy opis			**Parametry oferowane**
Serwer NAS			Producent: Model: Numer katalogowy (numer konfiguracji lub part numer):
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
1.	Procesor	4-rdzeniowy procesor ARM Cortex-A55 2.0 GHz	
2.	Wbudowana pamięć RAM	4GB	
3.	Maks. wielkość pamięci	4GB	
4.	Rodzaj pamięci	On-board DDR4	
5.	Wbudowana pamięć flash	4 GB	
6.	Liczba zainstalowanych dysków twardych	0	
7.	Maks. liczba dysków	4	
8.		Wyposażony w min. 2 dyski o pojemności 4 TB każdy Typ dysku . dając łącznie min. 8 TB	
9.	Format szerokości	3,5" (LFF)	
10.	Interfejs dysku	SATA III - 6 Gb/s	
11.	Obsługa hot-swap dysków	Nie RAID Tak	
12.	Poziomy RAID	0 1 10	
13.	Architektura sieci	GigabitEthernet	
14.	Interfejs sieciowy	sieciowy - 1 x 10/100/1000/2500 Mbit/s 2 x RJ-45 LAN Gniazda we/wy	
15.	USB	1 x USB 3.0 2 x USB 2.0	
16.	Liczba wentylatorów	1 Wentylator 12 cm Obudowa Tower	
17.	Zasilanie	Zasilacz 90W (12 VDC), 100-240 VAC	

Tabela nr 3

Szczegółowy opis			**Parametry oferowane**
Komputer stacjonarny typu All in One. W ofercie wymagane jest podanie modelu, symbolu oraz producenta			Producent: Model: Numer katalogowy (numer konfiguracji lub part numer):
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
1.	Procesor	Min. 6-rdzeniowy, zaprojektowany do komputerów stacjonarnych, zaoferowany procesor musi uzyskiwać w teście Passmark CPU Mark średni wynik minimum 10420 punktów na dzień 18.03.2022. Lista wyników testów w załączniku.	Spełnia / nie spełnia Model procesora:
2.	Pamięć operacyjna	1 x 8GB możliwość rozbudowy do min 64GB, minimum jeden slot wolny na dalszą rozbudowę	Spełnia / nie spełnia
3.	Parametry pamieci masowej	Min. 256 GB M.2 PCIe NVMe	Spełnia / nie spełnia
4.	Grafika	Zintegrowana z procesorem, ze wsparciem dla DirectX 12, OpenGL 4.5, osiągająca w teście Average G3D Mark wynik na poziomie *1200* punktów. Do oferty należy dołączyć wydruk ze strony: http://www.videocardbenchmark.net potwierdzający spełnienie wymogów SIWZ	Spełnia / nie spełnia Model karty graficznej:
5.	Wyposażenie multimedialne	karta dźwiękowa zintegrowana z płytą główną; wbudowane dwa głośniki stereo o mocy 2W na kanał.	Spełnia / nie spełnia
6.	Obudowa	Obudowa typu All in One -zintegrowany komputer w obudowie wraz z monitorem z matrycą IPS min 23,8" o parametrach: - rozdzielczość min 1920 x 1080 @60 Hz - kontrast typowy min 1000:1, - typowa jasność min 250 cd/m2, matryca matowa - kąty widzenia pion/poziom: min 178/178 stopni - kąty pochylenia w pionie min -5/+20 stopni - regulacja wysokości do 108 mm - Swivel +/- 45 stopni Waga max 7.80	Spełnia / nie spełnia

		Wymiary bez podstawy: 54 x 36 cm Posiadająca min. 1 wewnętrzną półkę 2,5" umożliwiającą zamontowanie dysku 2,5" (HDD/SSD/SED).	
7.		Zaprojektowana i wykonana przez producenta komputera opatrzona trwałym logo producenta. Wymagany jest wbudowany fabrycznie dźwiękowo-wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, który musi sygnalizować co najmniej: - awarie procesora - uszkodzenie kontrolera Video - uszkodzenie pamięci RAM Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) Zasilacz zewnętrzny o mocy max: 120W o sprawności min 89% Komputer musi być wyposażony w menu ekranowe z poziomu którego użytkownik może ustawić jasność, kontrast oraz włączyć technologie obniżającą poziom niebieskiego światła (tzw Low Blue Light) oraz tryb nocny (tzw Night Light).	
8.	Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z wymaganym systemem operacyjnym (załączyć wydruk ze strony Microsoft WHCL). Dopuszcza się wydruk w języku angielskim.	Spełnia / nie spełnia
9.	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 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 Możliwość wyłączenia/włączenia: zintegrowanej karty sieciowej, kontrolera audio, serial portu, portów USB (bok, tył), funkcjonalności ładowania zewnętrznych urzadzeń przez port USB, poszczególnych slotów SATA, czytnika kart SD, audio, funkcji TurboBoost, wirtualizacji 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. BIOS musi posiadać funkcję update BIOS z opcją automatycznego 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. Diagnostyka uruchamiana z BIOS działająca bez obecności systemu operacyjnego czy dysku twardego umożliwiająca na przeprowadzenie testów diagnostycznych w tym m.in.: – test procesora	Spełnia / nie spełnia

		– test dysku twardego – test pamięci RAM – test płyty głównej	
10.	Bezpieczeństwo	1. BIOS musi posiadać możliwość – 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, – możliwość ustawienia hasła na dysku (drive lock) – blokady/wyłączenia portów USB, COM, karty sieciowej, karty audio; – kontroli sekwencji boot-ącej; – startu systemu z urządzenia USB – funkcja blokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń 2. Komputer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (TPM v 2.0); 3. Możliwość zapięcia linki typu Kensington i kłódki do dedykowanego oczka w obudowie komputera 4. Czujnik otwarcia obudowy zintegrowany trwale z płytą główną i zarządzany z poziomu BIOS w zakresie min włączyć/wyłączyć. 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: - informacje o systemie, min.: 1. Procesor: typ procesora, jego obecną 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. 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	Spełnia / nie spełnia
11.	Certyfikaty i standardy	– Certyfikat ISO 9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu). Dopuszcza się wersję w języku angielskim. – Deklaracja zgodności CE (załączyć do oferty). Dopuszcza się wersję w języku angielskim.	Spełnia / nie spełnia

		– Komputer musi spełniać wymogi normy Energy Star min 7.0 Wymagany certyfikat lub wpis dotyczący oferowanego modelu komputera w internetowym katalogu http://www.energystar.gov - dopuszcza się wydruk ze strony internetowej. Dopuszcza się wersję w języku angielskim.	
12.		– Komputer musi spełniać wymogi dla TCO Edge - dopuszcza się wydruk ze strony https://tcocertified.com/ . Dopuszcza się wydruk w języku angielskim.	
13.	Ergonomia	Maksymalnie 18 dB z pozycji operatora w trybie IDLE, pomiar zgodny z normą ISO 9296 / ISO 7779; wymaga się dostarczenia odpowiedniego certyfikatu lub deklaracji producenta. Dopuszcza się wersję w języku angielskim.	Spełnia / nie spełnia
14.	Warunki gwarancji	3 letnia gwarancja producenta. Oświadczenie producenta potwierdzające w/w wymóg gwarancyjny.	Spełnia / nie spełnia
15.	Wsparcie techniczne producenta	Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera (ogólnopolski numer - w ofercie należy podać numer telefonu) 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) – czasu obowiązywania i typ udzielonej gwarancji 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 Możliwość weryfikacji czasu obowiązywania i reżimu gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera	Spełnia / nie spełnia
16.	Wymagania dodatkowe	1. Zainstalowany system operacyjny umożliwiający szyfrowanie danych, pracę grupową oraz pracę w domenie; nie dopuszcza się w tym zakresie licencji oraz nośników pochodzących z rynku wtórnego. Licencja systemu operacyjnego zaimplementowana w BIOS komputera, umożliwiająca instalację systemu bez podawania klucza oraz bez aktywacji systemu za pośrednictwem Internetu. **Nie dopuszcza się licencji edukacyjnej** 2. Wbudowane porty i złącza:- porty wideo: min. 1 szt DisplayPort 1.4 (DP++), HDMI-in - 1.4 oraz: *1 szt HDMI 2.0 lub 1 szt* Display Port 1.4 - min. 6 x USB w tym min: 1 szt USB 3.2 Gen 2 Typ-C o przepustowości do 10 Gbps z boku obudowy, 1 szt USB 3.2 Gen 2 Typ-A o przepustowości do 10 Gbps z boku obudowy, 4 szt USB 3.2 Gen 1 Typ-A o przepustowości do 5Gbps z tyłu obudowy, - port sieciowy RJ-45 - port audio COMBO - chroniąca przed wizualnym hackingiem chowana w obrysie komputera kamera internetowa: 5 MP RGB z dwoma mikrofonami;	Spełnia / nie spełnia Podać nazwę i wersję systemu:

		Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera)portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, adapterów itp. 3. Karta sieciowa 10/100/1000 Ethernet RJ 45 (zintegrowana) z obsługą PXE, WoL, 4. Karta WiFi AX Wireless 2x2 z Bluetooth 5.0 M.2 5. Płyta główna, wyposażona w: - 2 złącza SODIMM z obsługą do 64GB pamięci RAM - 1 złącze M.2 PCIe x1 dla WLAN - 1 złącze M.2 PCIe x4 dla dyskuSSD - 1 złącze SATA dla dysku 2,5" 6. Klawiatura USB w układzie polski programisty 7. Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll) 8. Napęd optyczny SLIM	

Tabela nr 4

Szczegółowy opis			**Parametry oferowane**
UTM			Producent: Model: Numer katalogowy (numer konfiguracji lub part numer):
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
1.	OBSŁUGA SIECI	1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, fi rewa II, systemu IPS oraz usług sieciowych takich jak np. DHCP.	
2.	ZAPORA KORPORACYJNA (Firewall)	2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 3. Urządzenie ma obsługiwać translacje adresów NAT n:l, NAT 1:1 oraz PAT.	

		4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).	
3.	INTRUSION PREVENTION SYSTEM (IPS)	12. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 13. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 14. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 15. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 16. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 17. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.	

		18. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. 19. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 20. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose &SV).	
4.	KSZTAŁTOWANIE PASMA (Traffic Shapping)	21. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 22. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 23. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). 24. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.	
5.	OCHRONA ANTYWIRUSOWA	25. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 26. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 27. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 28. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.	
6.	OCHRONA ANTYSPAM	29. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 30. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNSRBL,	

		c. Skaner heurystyczny. 31. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. 32. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.	
7.	WIRTUALNE SIECI PRYWATNE (VPN)	33. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny- lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 34. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: a. PPTPVPN, b. IPSecVPN, c. SSLVPN. 35. SSL VPN ma działać co najmniej w trybach tunelu i portalu. 36. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. 37. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 38. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. 39. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.	
8.	FILTR DOSTĘPU DO STRON WWW	40. Urządzenie ma posiadać wbudowany filtr URL. 41. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 42. Administrator ma mieć możliwość dodawania własnych kategorii URL. 43. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 44. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 45. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. 46. Filtr URL musi uwzględniać komunikację po protokole HTTPS.	

		47. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 48. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.	
9.	UWIERZYTELNIANIE	49. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 50. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. 51. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. 52. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. 53. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. 54. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.	
10.	ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)	55. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 56. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 57. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 58. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).	

		59. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. 60. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 61. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.	
11.	ROUTING (TRASOWANIE)	62. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 63. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 64. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). 65. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.	
12.	ADMINISTRACJA URZĄDZENIEM	66. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 67. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS. 68. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 69. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 70. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH) 71. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 72. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 73. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 74. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. 75. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: a. manualnego eksportu do pliku w dowolnym momencie czasu, b. automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu	

		76. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. 77. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.	
13.	RAPORTOWANIE	78. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 79. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 80. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 81. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. 82. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 83. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 84. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 85. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).	
14.	POZOSTAŁE USŁUGI I FUNKCJE	86. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. 87. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 88. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 89. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci w zakresie określenia bramy, serwerów DNS, nazwy domeny. 90. Urządzenie ma posiadać usługę DNS Proxy. 91. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwezsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.	

15.	GWARANCJA I SERWIS	92. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. 93. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.	
16.	PARAMETRY SPRZĘTOWE	94. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. 95. Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów. 96. Liczba portów Ethernet 10/100/lOOOMbps - min.8. 97. Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 98. Przepustowość Firewall (1518 bajtów UDP) - minimum 2Gbps. 99. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) - minimum 1.6Gbps. 100. Przepustowość filtrowania Antywirusowego - minimum 400Mbps. 101. Przepustowość tunelu VPN przy szyfrowaniu AES - minimum 350Mbps. 102. Maksymalna liczba tuneli VPN IPSec - minimum 50. 103. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) - minimum 20. 104. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) - minimum 20. 105. Obsługa interfejsów 802.llq (VLAN) - minimum 128 106. Liczba równoczesnych sesji - minimum 200 000 i nie mniej niż 15 000 nowych sesji/sekundę. 107. Urządzenie nie ma limitu na liczbę użytkowników. 108. Liczba reguł filtrowania - minimum 4 096. 109. Liczba tras statycznego routingu - minimum 512. 110. Liczba tras dynamicznego routingu - minimum 10 000.	

Tabela nr 5

Szczegółowy opis			**Parametry oferowane**
UPS			Producent: Model: Numer katalogowy (numer konfiguracji lub part numer):
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
1.	Zasilacz awaryjny UPS	- Moc rzeczywista: min. 300 Wat - Maks. czas przełączenia na baterię: 5 ms - Liczba i rodzaj gniazdek z utrzymaniem zasilania: 4 x IEC320 C13 (10A) - Typ gniazda wejściowego: IEC320 C14 (10A) - Czas podtrzymania dla obciążenia 100%: 3 min - Czas podtrzymania przy obciążeniu 50%: 7 min - Zakres napięcia wejściowego w trybie podstawowym: 170-264 V - Zimny start: Tak - Układ automatycznej regulacji napięcia (AVR) - Alarmy dźwiękowe: praca z baterii - Wyposażenie standardowe: przewód zasilający	

Tabela nr 6

Szczegółowy opis			**Parametry oferowane**
Program Antywirusowy			Producent: Model: Numer katalogowy (numer konfiguracji lub part numer):
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
1.	**Administracja zdalna**	1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD. 2. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL 3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. 4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. 5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów. 6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. 7. Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android. 8. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci. 9. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).	

		10. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. 11. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 12. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 13. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 14. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora. 15. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. 16. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.	
2.	**Ochrona stacji roboczych**	1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.l/Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.	

		7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IM APS. 12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne -jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej lub obu metod jednocześnie. 13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,	

		• tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego MS Outlook. 23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: • tryb automatyczny - rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, • tryb interaktywny - rozwiązanie pyta się o każde nowo nawiązywane połączenie, • tryb oparty na regułach - rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, • tryb uczenia się - rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. 24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. 25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.	

		27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. 28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.	
3.	**Ochrona serwera**	1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne -jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie-z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.	
4.	Dodatkowe wymagania dla ochrony serwerów Windows:	9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.	

		14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.	
5.	Dodatkowe wymagania dla ochrony serwerów Linux:	18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.	
6.	Ochrona urządzeń mobilnych opartych o system Android	22. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 23. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 24. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 25. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. 26. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: a. usunięcie zawartości urządzenia, b. przywrócenie urządzenie do ustawień fabrycznych, c. zablokowania urządzenia,	

		d. uruchomienie sygnału dźwiękowego, e. lokalizację GPS. 27. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 28. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: a. nazwę aplikacji, b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła	

Tabela nr 7

Szczegółowy opis			**Parametry oferowane**
Oprogramowanie biurowe			Producent: Model: Numer katalogowy (numer konfiguracji lub part numer):
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
1.	Zintegrowany, pakiet aplikacji biurowych zawierający min:	- interfejs w języku polskim, - w skład pakietu musi wchodzić co najmniej: a) procesor tekstu, b) arkusz kalkulacyjny, c) program do tworzenia prezentacji, d) program do obsługi poczty z kalendarzem e) program do tworzenia cyfrowych notatek - procesor tekstu musi posiadać pełną zgodność z formatami plików .doc, .docx oraz możliwość zapisu pliku do .pdf,	

		- arkusz kalkulacyjny musi posiadać pełną zgodność z formatami plików .xls, .xlsx oraz możliwość zapisu pliku do .pdf, - program do tworzenia prezentacji musi posiadać pełną zgodność z formatami plików .ppt, pptx, oraz możliwość zapisu pliku do .pdf, - program do obsługi poczty musi posiadać pełną zgodność z formatami plików .msg, - program do tworzenia cyfrowych notatek musi posiadać pełną zgodność z formatami plików .one oraz możliwość zapisu pliku do .pdf, - pakiet musi posiadać pełną integralność pomiędzy składnikami (kopiuj-wklej wraz z możliwością wyboru sposobu wklejenia zawartości), - pakiet musi posiadać możliwość uruchamiania i tworzenia makropoleceń w języku Visual Basic for Applications.	
2.	Licencja	Licencja wieczysta na jedno stanowisko , nieograniczona czasowo. Nie dopuszcza się oprogramowania stworzonego na podstawie darmowego kodu Open Source.	

Tabela nr 8

Szczegółowy opis			**Parametry oferowane**
Oprogramowanie OCR			Producent: Model: Numer katalogowy (numer konfiguracji lub part numer):
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**	**Parametry**
1.	Oprogramowanie OCR	1. Licencja: min. 3-letnia, ESD 2. Liczba użytkowników: 1 3. Digitalizacja dokumentów 4. Odzyskiwanie dokumentów 5. Edytowanie dokumentów 6. Udostępnianie dokumentów	

		7. Zabezpieczenia dokumentów 8. Obsługa dokumentów PDF zgodnie ze specyfikacją ISO Konwertowanie dokumentów PDF do formatów aplikacji biurowych Poprawianie całych zdań i akapitów dokumentów PDF 9. Możliwość zmiany formatu, czcionki, koloru, odstępów międzyznakowych dla całego akapitu lub dla fragmentów tekstu 10. Zmiana układu dokumentów PDF 11. Natychmiastowe rozpoznawanie w tle umożliwiające bezpośrednią pracę z nieprzeszukiwalnymi dokumentami PDF 12. Duża liczba języków rozpoznawania, w tym inteligentne wykrywanie języka dokumentu i obsługa dokumentów wielojęzycznych 13. Obsługa formuł chemicznych i edytowanie tabel (komórki edytowalne pojedynczo, bez wpływu na pozostałe części tabeli) 14. Zapisywanie dokumentów PDF 15. Możliwość edytowania dokumentów PDF, możliwość nanoszenia uwag, formatowania tekstu bezpośrednio w formacie PDF 16. Zachowywanie kolorów tekstów	