Załącznik nr 2.

Szczegółowy opis przedmiotu zamówienia / Oferowane parametry techniczne sprzętu

Dostaw sprzętu komputerowego i oprogramowania w ramach projektu Cyfrowa Gmina.

1. Przedmiotem zamówienia jest: Zakup sprzętu komputerowego i oprogramowania w ramach projektu „Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU".

2. Przedmiot zamówienia został podzielony na 2 cześci :

Część 1. – Zakup sprzętu i oprogramowania komputerowego w ramach projektu „Cyfrowa Gmina", w zakres której wchodzi dostawa:

1.1 Komputer stacjonarny typu All In One – 19 szt.

1.2 Zasilacz awaryjny do komputera stacjonarnego (UPS) - 19 szt.

1.3 Komputer przenośny laptop - 2szt.

1.4 Urządzenie wielofunkcyjne (Drukarka, Kopiarka, Skaner) – 1 szt.

1.5 Oprogramowanie MS Office 2021 Home&Business PL – 25 szt.

Część 2. – Zakup Urządzenia zapory sieciowej typu UTM w ramach projektu „Cyfrowa Gmina", w zakres której wchodzi dostawa:

2.1 Urządzenie zapory sieciowej typu UTM z wdrożeniem – 1 szt.

Niniejszy załącznik stanowi jednocześnie szczegółowy opis przedmiotu zamówienia. Zaoferowany przez Wykonawcę sprzęt komputerowy i oprogramownie musi spełniać minimalne wymagania postawione w niniejszym załączniku w kolumnie „Wymagane minimalne parametry techniczne " oraz zostać dostarczony na warunkach określonych poniżej. Wykonawca zobowiązany jest podać też producenta, model oferowanego sprzętu, typ. Dodatkowo Zamawiający dopuszcza podanie linków dostępowych dla oferowanego n/w sprzętu dostępnych na stronach internetowych producentów.

Wykonawca może złożyć ofertę na dwie części zamówienia lub na dowolnie wybraną część zamówienia.

Część 1. – Zakup sprzętu i oprogramowania komputerowego w ramach projektu „Cyfrowa Gmina", w zakres której wchodzi dostawa:

1.1 Komputer stacjonarny typu All In One – 19 szt.

1.2 Zasilacz awaryjny do komputera stacjonarnego (UPS) - 19 szt.

1.3 Komputer przenośny laptop - 2szt.

1.4 Urządzenie wielofunkcyjne (Drukarka, Kopiarka, Skaner) – 1 szt.

1.5 Oprogramowanie MS Office 2021 Home&Business PL – 25 szt.

1.1 Stacje robocze - Komputer stacjonarny All in One – 19 sztuk

Producent: ……

Model: ……

Numer katalogowy (numer konfiguracji): ……..

Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Ekran	Przekątna: min 23,8" Rozdzielczość: min. FHD (1920x1080) IPS, Matryca: Jasność typowa min. 250 cd/m², Kontrast typowy 1000:1 Barwa koloru (typowa) 72% NTSC, Kąty widzenia 178, Rodzaj matrycy Matowa IPS
Obudowa	– zintegrowana z monitorem (All in One) – musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona lub równoważne pozwalające na fizyczne zabezpieczenie urządzenia) – Obudowa trwale oznaczona nazwą producenta, nazwą komputera, part numberem, numerem seryjnym – Podstawa musi umożliwiać regulację kąta pionie w zakresie -5 do 20 stopni
Chipset	Dostosowany do zaoferowanego procesora
Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera Wyposażona w min. 2 złącza M.2 z czego jedno obsługujące dysk SSD PCIe NVMe
Procesor	Procesor dedykowany do pracy w komputerach stacjonarnych, 10 rdzeni, 12 wątków, 3.30-4.40 GHz, 12 MB cache, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 13382 punktów według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php
Pamięć operacyjna	16GB DDR4 3200 MHz możliwość rozbudowy do 32GB, jeden slot wolny
Dysk twardy	Dysk M.2 SSD 512GB PCIeNVMe Obudowa musi umożliwiać montaż dodatkowego dysku 2.5"

Napęd optyczny	Nie wymagany
Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia pamięci.
Audio/Video	Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo, wbudowane 2 mikrofony, wbudowana kamera 5 Mpx z wbudowaną przesłoną mechaniczną umożliwiającą jej fizyczne zasłonięcia i diodą LED informującą użytkownika o pracy, Możliwość podłączenia zewnętrznego monitora wraz ze wsparciem rozdzielczości 4K w min. 30Hz.
Karta sieciowa	Wi-Fi 6 (802.11 a/b/g/n/ac/ax), LAN 10/100/1000 Mbps, Bluetooth
Porty/złącza	Wbudowane (minimum): 2 x USB 3.2 Gen 1, 2 x USB-C 3.2 Gen 2, 1 x HDMI, 1 x słuchawki/mikrofon, 1 x LAN (Gigabit Ethernet). Wymagana ilość portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
Klawiatura/mysz	Klawiatura przewodowa USB Mysz przewodowa z rolką (scroll) USB
Zasilacz	Zasilacz o sprawności minimum 88% o mocy nie większej niż 65W.
System operacyjny	System operacyjny MS Windows 11 Pro 64-bit PL, tj.: (posiadający pełną funkcjonalność jaką oferuje podany w OPZ system operacyjny) z oryginalnym nośnikiem instalacyjnym lub kluczem licencyjnym umożliwiającym pobranie programu instalacyjnego ze strony producenta, zapewniający reinstalację, wsparcie dla Active Directory i domeny. •Licencja powinna być nieograniczona w czasie, • Wykonawca zobowiązuje się dostarczyć niepowtarzalny (unikatowy) klucz do aktywacji dostarczonych licencji, • Oprogramowanie musi być fabrycznie nowe, objęte gwarancją oraz pochodzić z autoryzowanego kanału sprzedaży na rynek Unii Europejskiej, • Oprogramowanie nie może być wcześniej używane, regenerowane, serwisowane, rejestrowane ani aktywowane – Zamawiający zastrzega sobie prawo do weryfikacji czy dostarczone oprogramowanie (licencje) i powiązane z nimi elementy, takie jak certyfikaty/etykiety dołączone do oprogramowania są oryginalne, nowe i licencjonowane zgodnie z prawem oraz zasadami producenta oprogramowania, • Wykonawca zapewni kompatybilność (bezpieczeństwo, stabilność i wydajność) nowych komputerów z wykorzystywanymi przez zamawiającego rozwiązaniami (zwłaszcza w kontekście udziałów sieciowych i uprawnień do nich) w oparciu o system domen w środowisku LAN. Jeżeli ze względu na zaoferowane oprogramowanie zaistnieje konieczność poniesienia przez zamawiającego dodatkowych nakładów (w szczególności na zmianę konfiguracji usług sieciowych, szkolenie pracowników, zwiększenie dotychczasowej czasochłonności przygotowania stanowisk komputerowych) niezbędnych do sprawnego funkcjonowania stacji roboczych w infrastrukturze

	teleinformatycznej zamawiającego, wszelkie koszty z tym związane poniesie wykonawcą.
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: - modelu komputera, producencie komputera - numerze seryjnym, - numerze inwentarzowym, - MAC Adres karty sieciowej, - wersja Biosu wraz z datą produkcji, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem, - napędach lub dyskach podłączonych do portów SATA oraz M.2 (model dysku twardego i napędu optycznego) - o zainstalowanej licencji systemu operacyjnego na płycie głównej Możliwość z poziomu Bios: - wyłączenia selektywnego (pojedynczego) portów USB, - wyłączenia selektywnego (pojedynczego) portów SATA, - wyłączenia wbudowanej kamery, karty WiFi, karty audio, mikrofonu, głośników, czytnika kart - włączania/wyłączania trybu PXE - włączania/wyłączania obsługi TPM - włączania/wyłączania wirtualizacji oraz funkcji I/O - włączania/wyłączania funkcji Turbo procesora o ile ją obsługuje - ustawienia hasła: administratora, Power-On, HDD, - wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan) - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - zdefiniowania trzech sekwencji bootujących (podstawowa, WOL, po awarii) - załadowania optymalnych ustawień Bios
Certyfikaty i standardy	- Certyfikat ISO9001 dla producenta sprzętu - Energy Star

	- Deklaracja zgodności CE - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
rozmiary urządzenia/ szerokość, głębokość, wysokość, waga	54.062 cm - 18.37 cm - 41.901 cm , 5.37 kg - z podstawką
Bezpieczeństwo	Złącze typu Kensington Lock, Wbudowany moduł TPM
Gwarancja	3-letnia gwarancja producenta świadczona na miejscu u klienta. Czas reakcji serwisu - do końca następnego dnia roboczego Wymagane dołączenie do oferty oświadczenie producenta komputera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
Wsparcie techniczne producenta	Bezpośredni kontakt z Autoryzowanym Partnerem Serwisowym Producenta (brak konieczności zgłaszania każdej usterki sprzętowej telefonicznie), mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki. Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta. Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta.
Wymagania dodatkowe	Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej SIWZ. W tym celu Wykonawcy na wezwanie Zamawiającego dostarczą do siedziby Zamawiającego w terminie 5 dni od daty otrzymania wezwania, próbkę oferowanego sprzętu. W odniesieniu do programowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Ocena złożonych próbek zostanie dokonana przez Komisję Przetargową na zasadzie spełnia / nie spełnia. Z badania każdej próbki zostanie sporządzony protokół. Pozytywna ocena próbki będzie oznaczała zgodność próbki (oferty) z treścią SIWZ. Niezgodność próbki z SIWZ chociażby w zakresie jednego parametru podlegającemu badaniu bądź nieprzedłożenie wymaganej próbki w sposób i terminie wymaganym przez Zamawiającego będzie oznaczało negatywny wynik oceny próbki i będzie skutkowało odrzuceniem oferty na podstawie art. 89 ust. 1 pkt 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 ze zm.), tj. z uwagi na fakt, że treść oferty nie odpowiada treści specyfikacji istotnych warunków zamówienia. Szczegółowy sposób przygotowania i złożenia próbek zostanie dostarczony wykonawcom wraz z wezwaniem do złożenia próbek

1.2 Zasilacz awaryjny do komputera stacjonarnego (UPS) – 19 sztuk

Producent: ……

Model: ……

Numer katalogowy (numer konfiguracji): ……..

Parametry/Typ	**Wymagane minimalne parametry techniczne**
Moc pozorna	850 VA
Moc rzeczywista	480 W
Technologia	VI (line interactive)
Typ obudowy	wolnostojąca
WEJŚCIE	
Napięcie znamionowe (wartość skuteczna	230 V AC
Zakres napięcia wejściowego (wartości skuteczne) i tolerancja	170 ÷ 280 V AC ± 7 %
Częstotliwość znamionowa napięcia wejściowego 50 Hz Zakres częstotliwości i tolerancja	45 ÷ 55 Hz ± 1 Hz
Progi przełączania: sieć – UPS	170 ÷ 280 V AC ± 7 %
WYJŚCIE	
Napięcie znamionowe (wartość skuteczna)	230 V AC
Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa	230 V AC ± 10 %
Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca rezerwowa	230 V AC ± 10 %
Automatyczna regulacja napięcia (AVR)	+/- 10%
Kształt napięcia wyjściowego	Schodkowa aproksymacja sinusoidy / Tak jak na wejściu
Częstotliwość znamionowa napięcia wyjściowego	50 Hz
Zakres częstotliwości (tolerancja) – praca sieciowa	Synchronicznie z siecią
Zakres częstotliwości (tolerancja) – praca rezerwowa	50 Hz ± 1Hz

Filtracja napięcia wyjściowego	RC
Progi przełączania: UPS – sieć	176 V ÷ 274 V AC ± 7 %
Czas przełączenia na pracę rezerwową	< 6 ms
Czas powrotu na pracę sieciową	0 ms
AKUMULATORY I CZASY PODTRZYMANIA	
Akumulatory wewnętrzne	12 V / 9 Ah VRLA
Liczba akumulatorów wewnętrznych	1
Dopuszczalna całkowita pojemność akumulatorów wewnętrznych	9 Ah
Czas podtrzymania z baterii wewnętrznych (80 % / 50 % Pmax)	2 / 6 min
Napięcie nominalne obwodu DC	12 V DC
Maksymalny czas ładowania baterii wewnętrznych UPS - po 80% wyładowaniu baterii*	6 h
PARAMETRY TECHNICZNE	
Wymiary (wys. x szer. x gł.)	143 x 100 x 290 mm
Masa	5,2 kg
Zabezpieczenie wejściowe	Zabezpieczenie instalacji elektryczne
Zabezpieczenie wyjściowe	Elektroniczne – przeciwzwarciowe i przeciążeniowe
Przyłącze zasilania UPS	Przewód zakończony wtyczką z uziemieniem 16 A (PN-E-93201:1997) + uni-schuko
Przyłącza wyjściowe (liczba i typ gniazd)	2 x PN-E-93201
Sygnalizacja	Akustyczno – optyczna; wyświetlacz LCD
Interfejsy komunikacyjne	USB
Filtr telekomunikacyjny – RJ11	TAK
Deklaracje	CE
Normy	PN-EN 62040-1:2009, PN-EN 62040-2:2008
Gwarancja	24 miesiące

1.3 Komputer przenośny laptop - 2 sztuki

Producent: ……

Model: ……

Numer katalogowy (numer konfiguracji): ……..

Parametry/Typ	**Wymagane minimalne parametry techniczne**
Typ:	Komputer typu notebook z ekranem o przekątnej 17,3” i rozdzielczości nie mniejszej niż 1920 x 1080 pikseli (FullHD). Matryca wykonana w technologii IPS z powłoką antyrefleksyjną Jasność matrycy nie mniejsza niż 300 nitów, częstotliwość odświeżania matrycy 144 Hz matryca z pokryciem barw 100% sRGB
Procesor:	Procesor dedykowany do pracy w komputerach przenośnych, taktowany nominalnym zegarem, co najmniej 2,6 GHz, z pamięcią cache co najmniej 8 MB osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 11086 punktów według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php
Pamięć RAM:	DDR4 32 GB z pełnym wsparciem dla pamięci działających z taktowaniem 3200 MHz.
Pamięć operacyjna/ magazyn danych:	1000 GB M.2 NVMe PCIe 3.0 SSD. Możliwość dołożenia drugiego dysku pracującego w standardzie SATA lub NVMe bez utraty gwarancji.
Karta graficzna:	Dedykowana. Wielkość pamięci karty graficznej 4096 MB GDDR6 (pamięć własna) Powinna osiągać w teście wydajności: PassMarkPerformanceTest wynik min. 9162 punktów w G3D Mark (wynik dostępny: http://videocardbenchmark.net/gpu_list.php).
Multimedia:	Karta dźwiękowa zgodna z HD Audio. Wbudowane głośniki. Kamera 1.0 Mpix. Wbudowane dwa mikrofony
Łączność	Karta 802.11a/b/g/n/ac/ax + BlueTooth 5.2. Zintegrowana gigabitowa karta LAN – zamawiający nie dopuszcza możliwości zastosowania karty USB-LAN.
Bateria i zasilacz:	Minimum 3 komorowa o pojemności 4550 mah. Zasilacz dedykowany do notebooka - brandowany logo Producenta komputera.

Funkcje BIOS:	BIOS zgodny ze specyfikacją UEFI. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS bieżących informacji o: - numerze seryjnym komputera. - wersji BIOS. - ilości zainstalowanej pamięci RAM. - zastosowanym procesorze wraz z taktowaniem. - zamontowanym dysku twardym wraz z jego pojemnością i modelem.. Możliwość włączenia/wyłączenia zintegrowanego z komputerem touchpada. Możliwość włączenia/wyłączenia bezprzewodowej karty sieciowej i modułu BlueTooth. Możliwość włączenia/wyłączenia zintegrowanej karty LAN. Możliwość włączenia/wyłączenia karty dźwiękowej. Możliwość włączenia/wyłączenia zintegrowanej kamery. Możliwość włączenia/wyłączenia portów USB. Możliwość włączenia/wyłączenia modułu TPM. Możliwość ustawienia niezależnych haseł dla konta administratora, użytkownika i dysku twardego.
Certyfikaty i standardy:	Certyfikat ISO9001 dla producenta sprzętu Certyfikat ISO9001 dla autoryzowanego serwisu Producenta notebooka Certyfikat ISO 14001 dla producenta sprzętu. Deklaracja zgodności CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta sprzętu (załączyć do oferty oświadczenie Wykonawcy opatrzone numerem postępowania oraz poparte oświadczeniem Producenta potwierdzające spełnienie wymogu).
Waga i wymiary:	Waga nieprzekraczająca 2,80kg, wymiary WxSxG – 25,5 mm x 405 mm x 258 mm.
Bezpieczeństwo:	Dedykowana dioda LED zintegrowanej kamery sygnalizująca pracę komponentu. Zintegrowany z płytą główną moduł TPM.
Warunki gwarancji:	a) Gwarancja producenta komputera min 24 miesiące b) Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta c) Autoryzowany Partner Serwisowy musi posiadać status autoryzowanego partnera serwisowego e) Serwis urządzeń musi być realizowany zgodnie z wymogami normy ISO9001
Wsparcie techniczne producenta:	Możliwość sprawdzenia telefonicznego bezpośrednio u producenta oraz na stronie internetowej producenta oferowanego notebooka, po podaniu numeru seryjnego - konfiguracji sprzętowej notebooka oraz warunków gwarancji. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta notebooka, realizowany poprzez podanie na stronie internetowej producenta numeru seryjnego lub modelu notebooka

Porty	Min.: USB 3.2 – 3 szt. USB Type-C – 1 szt. RJ-45 (LAN) – 1 szt HDMI – 1 szt. DC-in (wejście zasilania) – 1szt. Wyjście słuchawkowe/wejście mikrofonowe – 1 szt. Czytnik kart pamięci SD - 1szt.
Klawiatura, touchpad	Z dedykowanym blokiem numerycznym po prawej stronie, podświetlona. Wielodotykowy, intuicyjny touchpad
System operacyjny	System operacyjny MS Windows 11 Pro 64-bit PL, tj.: (posiadający pełną funkcjonalność jaką oferuje podany w OPZ system operacyjny) z oryginalnym nośnikiem instalacyjnym lub kluczem licencyjnym umożliwiającym pobranie programu instalacyjnego ze strony producenta, zapewniający reinstalację, wsparcie dla Active Directory i domeny. •Licencja powinna być nieograniczona w czasie, • Wykonawca zobowiązuje się dostarczyć niepowtarzalny (unikatowy) klucz do aktywacji dostarczonych licencji, • Oprogramowanie musi być fabrycznie nowe, objęte gwarancją oraz pochodzić z autoryzowanego kanału sprzedaży na rynek Unii Europejskiej, • Oprogramowanie nie może być wcześniej używane, regenerowane, serwisowane, rejestrowane ani aktywowane – Zamawiający zastrzega sobie prawo do weryfikacji czy dostarczone oprogramowanie (licencje) i powiązane z nimi elementy, takie jak certyfikaty/etykiety dołączone do oprogramowania są oryginalne, nowe i licencjonowane zgodnie z prawem oraz zasadami producenta oprogramowania, • Wykonawca zapewni kompatybilność (bezpieczeństwo, stabilność i wydajność) nowych komputerów z wykorzystywanymi przez zamawiającego rozwiązaniami (zwłaszcza w kontekście udziałów sieciowych i uprawnień do nich) w oparciu o system domen w środowisku LAN. Jeżeli ze względu na zaoferowane oprogramowanie zaistnieje konieczność poniesienia przez zamawiającego dodatkowych nakładów (w szczególności na zmianę konfiguracji usług sieciowych, szkolenie pracowników, zwiększenie dotychczasowej czasochłonności przygotowania stanowisk komputerowych) niezbędnych do sprawnego funkcjonowania stacji roboczych w infrastrukturze teleinformatycznej zamawiającego, wszelkie koszty z tym związane poniesie wykonawcą.
Wymagania dodatkowe	Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej SIWZ. W tym celu Wykonawcy na wezwanie Zamawiającego dostarczą do siedziby Zamawiającego w terminie 5 dni od daty otrzymania wezwania, próbkę oferowanego sprzętu. W odniesieniu do programowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Ocena złożonych próbek zostanie dokonana przez Komisję Przetargową na zasadzie spełnia / nie spełnia. Z badania każdej próbki zostanie sporządzony protokół. Pozytywna ocena próbki będzie oznaczała zgodność próbki (oferty) z treścią SIWZ. Niezgodność próbki z SIWZ chociażby w zakresie jednego parametru podlegającemu badaniu bądź nieprzedłożenie wymaganej próbki w sposób i terminie wymaganym przez Zamawiającego będzie oznaczało negatywny wynik oceny próbki i będzie skutkowało odrzuceniem oferty na podstawie art. 89 ust. 1 pkt 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 ze zm.), tj. z uwagi na fakt, że treść oferty nie odpowiada treści specyfikacji istotnych warunków zamówienia. Szczegółowy sposób przygotowania i złożenia próbek zostanie dostarczony wykonawcom wraz z wezwaniem do złożenia próbek

Akcesoria	Torba na laptopa, Kompatybilność 17,3"

1.4 Urządzenie wielofunkcyjne (Drukarka, Kopiarka, Skaner) – 1 sztuka

Producent: ……

Model: ……

Numer katalogowy (numer konfiguracji): ……..

Parametry/Typ	**Wymagane minimalne parametry techniczne**
Typ	urządzenie wielofunkcyjne
Funkcje	Drukowanie, kopiowanie, skanowanie
Technologia druku	laserowa
Rodzaj	monochromatyczna
Rozmiar nośnika	A4
Pojemność podajnika papieru	250 szt.
Pojemność odbiornika papieru	150 szt.
Automat. druk dwustronny (dupleks)	tak
Interfejs	Ethernet 10/100/1000 Mbps , USB 2.0 , Wi-Fi
Zainstalowana pamięć	512 MB
Maks. pojemność pamięć	512 MB
Prędkość procesora	1200 MHz
Wspierane aplikacje mobilne	Android iOS
Obsługiwane systemy operacyjne	Windows - Windows Client OS (32/64-bitowy), Win10, Win8.1, Win 8 Basic, Win8 Pro, Win8 Enterprise, Win8 Enterprise N, Win7 Starter Edition SP1, UPD Win7 Ultimate Mac OS - Mac, Apple macOS Sierra v10.12, Apple macOS High Sierra v10.13, Apple macOS Mojave v10.14

	inne Mobile OS, iOS, Android
Przewód do połączenia z komputerem w zestawie	tak
Drukowanie	
Rozdzielczość druku w czerni	1200 x 1200 dpi
Maks. szybkość druku mono	38 str./min.
Szybkość druku dwustronnego	31 obr./min.
Minimalne zalecane obciążenie	750 str./mies.
Maksymalne obciążenie	80000 str./mies.
Czas do pierwszego druku monochromatycznego	6.3 s
Obsługiwane języki	HP PCL 5c , HP PCL 6 , Native Office , PDF , PWG , URF
Emulacje języków	PostScript v3
Skanowanie	
Typ skanera	CIS (płaski | kolorowy)
Rozdzielczość skanera	1200 x 1200 dpi
Maks. format skanu	A4
Obszar skanowania	216 x 297 mm
Szybkość skanowania arkuszy A4	2 s (monochromatyczne)
Kopiowanie	
Rozdzielczość kopiarki	600 x 600 dpi
Maksymalne wielokrotne kopiowanie	999 kopii
Eksploatacja	
Ilość pojemników na toner	1 szt.

Gramatura papieru	60 - 120 g/m²
Symbol tonera	HP No. 59A, HP No. 59X
Komunikacja	
Praca w sieci [serwer druku]	tak
Wyświetlacz	tak (dotykowy | kolorowy | przekątna: 6.86 cm)
Wymiary	
Szerokość, Głębokość, Wysokość	420 mm, 390 mm, 323 mm,
Waga	12.6 kg
Gwarancja	1 rok

1.5 Oprogramowanie Microsoft Office 2021 Home&Business PL – 25 sztuk

Oprogramowanie biurowe	Zintegrowany pakiet aplikacji biurowych musi zawierać co najmniej: - edytor tekstów - arkusz kalkulacyjny - narzędzie do przygotowywania i prowadzenia prezentacji - narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) - zainstalowanie na jednym komputerze produktów pochodzących od różnych producentów nie jest uznane za ofertę zintegrowanego pakietu. Pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. Pakiet biurowy powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim Dostępność w internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze. Pakiet musi mieć publicznie znany cykl życia przedstawiony przez producenta, dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa- co najmniej na 5 lat od daty zakupu. Możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0)

	Pakiet aplikacji biurowych powinien obsługiwać formaty dokumentów wymienione w Krajowych Ramach Interoperacyjności. Pakiet aplikacji biurowych powinien prawidłowo współpracować z aplikacjami w modelu chmury obliczeniowej, w szczególności do pracy grupowej i synchronizacji danych. Rozpoznawanie sieci i ich ustawienia bezpieczeństwa, rozpoznawać automatycznie urządzenia peryferyjne działające w tej sieci (np. drukarki, tablice interaktywne) oraz łączyć się automatycznie z raz zdefiniowanymi sieciami

Część 2. – Zakup sprzętu i oprogramowania komputerowego w ramach projektu „Cyfrowa Gmina", w zakres której wchodzi dostawa:

2.1 Urządzenie zapory sieciowej typu UTM z wdrożeniem – 1 sztuka

Producent: ……

Model: ……

Numer katalogowy (numer konfiguracji): ……..

Parametry/Typ	**Wymagane minimalne parametry techniczne**
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 aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. 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. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 5 portami Gigabit Ethernet RJ-45. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe:	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.
Funkcje Systemu Bezpieczeństwa:	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. 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. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. 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).
Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. 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. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.
Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

	• 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. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • 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.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. 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. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. 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. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

	10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. 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).
Kontrola WWW	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. 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. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. 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. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1. 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. 2. 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. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Certyfikaty	Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje: - ICSA lub EAL4 dla funkcji Firewall.

Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: 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 24 miesięcy.
Gwarancja oraz wsparcie	1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 24 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.
Rozszerzone wsparcie serwisowe AHB/SOS	System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 24 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7 Wymagania powinny być potwierdzone dokumentami: • Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 podmiotu serwisującego.
Wdrożenie	Wdrożenie podstawowe obejmuje: 1.Rejestracja urządzeń oraz licencji, 2.Aktualizacja oprogramowania oraz zmiana danych dostępowych (autoryzacja) do urządzeń, 3.Konfiguracja metod dostępu do urządzeń (SSH, HTTPS itp.) oraz autentykacji 2-poziomowej, 4.Konfiguracja łącz dostępowych do Internetu, łącz zapasowych oraz redundancji (WAN) 5.Segmentacja sieci LAN na urządzeniach (konfiguracja poszczególnych interfejsów sieciowych, konfiguracja Vlan) oraz polityk dostępu do poszczególnych podsieci/vlan'ów, 6.Uruchomienie serwerów DHCP na poszczególnych podsieciach/vlan'ach, 7.Konfiguracja routingu, agregacji portów 8.Konfiguracja polityk bezpieczeństwa (filtrowanie/blokowanie treści i aplikacji internetowych, antywirus, filtr DNS, IPS, usługa DLP,) 9.Integracja z domeną 10.Konfiguracja powiadomień e-mail, 11.Konfiguracja SNMP, 12.Konfiguracja procesu logowania (zawartość logów, okres przechowywania), 13.Wykonanie kopii zapasowej ustawień urządzeń. 14.Konfiguracja tuneli VPN IPSEC / SSL
Opisy do wymagań ogólnych	1. 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. 2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

Podsumowanie wyceny sprzętu i oprogramowania:

Lp	Asortyment	Cena jednostkowa netto	Cena łączna netto
Część 1. – Zakup sprzętu i oprogramowania komputerowego w ramach projektu „Cyfrowa Gmina			
1.1	Stacje robocze - Komputer stacjonarny typu All In One – 19 szt.		
1.2	Zasilacz awaryjny do komputera stacjonarnego (UPS) - 19 szt.		
1.3	Komputer przenośny laptop typu netebook - 2 szt.		
1.4	Urządzenie wielofunkcyjne (Drukarka, Kopiarka, Skaner) – 1 szt.		
1.5	Oprogramowanie MS Office 2021 Home&Business PL – 25 szt.		
		Suma netto	
		Podatek VAT	
		Kwota brutto	
Część 2. – Zakup Urządzenia zapory sieciowej typu UTM w ramach projektu „Cyfrowa Gmina”			
2.1	Urządzenie zapory sieciowej typu UTM z wdrożeniem – 1 szt.		
		Suma netto	
		Podatek VAT	
		Kwota brutto	

Kwoty za poszczególne części zamówienia należy przenieść do formularza ofertowego.

……

Podpis wykonawcy