IRŚ. 271.1.22.2022

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

na zadanie pn.: *„Dostawa sprzętu i oprogramowania komputerowego w ramach projektu Cyfrowa Gmina z podziałem na części”*

Przedbórz, dnia 12.01.2023 r.

Znak sprawy: **IRŚ.271.1.22.2022**

Dotyczy: postępowania prowadzonego w trybie podstawowym na podstawie art. 275 pkt. 1 pn.: ***„Dostawa sprzętu i oprogramowania komputerowego w ramach projektu Cyfrowa Gmina z podziałem na części”***

MODYFIKACJA

SPECYFIKACJI WARUNKÓW ZAMÓWIENIA

I. Zamawiający Gmina Przedbórz działając na podstawie art. 286 ust. 1 ustawy Prawo zamówień publicznych informuje, że zmienia:

1) załącznik nr 1a), który otrzymuje brzmienie:

Załącznik nr 1a do SWZ
Informacja o parametrach oferowanego przedmiotu zamówienia część I
Część I zakup i dostawa w ramach wydatków bieżących:
- urządzeń podtrzymujących napięcia serwer – UPS,
- stacji roboczych wraz z monitorami,
- oprogramowania do tworzenia kopii zapasowych,
- usług informatycznych w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania,
- rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS).

1. Przedmiot zamówienia obejmuje dostawę następującego sprzętu o parametrach nie gorszych niż wskazane poniżej:

1.1. Zakup urządzenia podtrzymującego napięcie serwera – UPS
Ilość: 1 szt.

Parametr	**Charakterystyka (wymagania minimalne)**	**Należy wpisać tak lub nie**
Główne napięcie wejściowe	208 V, 230 V	
Inne napięcie wejściowe	220 V, 240 V	
Główne napięcie	230 V	

wyjściowe		
Inne napięcie wyjściowe	208 V, 220 V, 240 V	
Moc znamionowa w W	2700 W	
Moc znamionowa w VA	3000 VA	
Typ podłączenia wejściowego	BS1363A Brytyjski, IEC 320 C20, Schuko CEE 7 / EU1-16P	
Liczba gniazd zasilających	8 IEC 320 C13, 2 IEC Jumpers, 1 IEC 320 C19	
Liczba szaf rackowych	2U	
Długość kabla	2,44 m	
Liczba kabli	1	
Rodzaj akumulatora	Akumulator kwasowo-ołowiowy	
Dostarczane wyposażenie	CD z oprogramowaniem, Wsporniki montażowe do szaf przemysłowych Kabel do sygnalizacji RS-232 do Smart-UPS Czujnik temperatury, podręcznik użytkownika, Karta do zdalnego zarządzania Web SNMP Management Card	
Ogólny		
Number of power module	2400	
Liczba slotów wypełnionych modułami mocy	0	
Liczba pustych slotów na moduły mocy	0	
Product web sub-family	Network card pre-installed	
Nadmiarowość	No	
Parametry fizyczne		
Kolor	Czarny	

IRŚ. 271.1.22.2022

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

na zadanie pn.: *„Dostawa sprzętu i oprogramowania komputerowego w ramach projektu Cyfrowa Gmina z podziałem na części”*

Wysokość	8,5 cm	
Szerokość	43,2 cm	
Głębokość	66,7 cm	
Masa produktu	37,32 kg	
Miejsce montażu	Przednie	
Sposób montażu	W szafie rackowej	
Możliwość montażu na dwóch słupkach	0	
Kompatybilność z USB	Tak	
Na wejściu		
Ograniczenie napięcia wejściowego	140...280 V	
Częstotliwość sieciowa	50/60 Hz +/- 3 Hz auto-sensing	
Na wyjściu		
Zniekształcenia harmoniczne	Poniżej 5 %	
Maksymalna możliwa do konfiguracji moc (w VA)	3000 VA	
Maksymalna możliwa do konfiguracji moc (w watach)	2700 W	
Czas przełączenia zasilania	2-4 ms, Zazwyczaj 6 ms, maksymalnie 10 ms	
Topologia	Line interactive	
Typ przebiegu	Sinusoida	
Częstotliwość wyjściowa	50/60 Hz +/- 3 Hz synchronicznie z siecią	
Certyfikaty i zgodność z normami		
Certyfikaty produktu	C-Tick CE EAC GOST IRAM VDE	
Parametry		

środowiskowe		
Poziom dźwięku	55 dBA	
Rozpraszanie ciepła	184 Btu/h	
Temperatura otoczenia dla pracy urządzenia	0...40°C	
Temperatura otoczenia dla przechowywania	15...45°C	
Wilgotność względna	0…95 %	
Wilgotność względna (przechowywanie)	0…95 %	
Akumulatory i czas podtrzymania		
Rozszerzalny czas podtrzymania	1	
Wstępnie zainstalowane baterie	0	
Puste gniazda akumulatorowe	0	
Typowy czas pełnego ładowania akumulatora	3 godz.	
Ilość zestawów RBC™	1	
Żywotność akumulatora	3…5 rok	
Moc baterii w VAH	738 VAh runtime	
Moc akumulatora (W)	245 W rated	
Opcja baterii	SMX120RMBP2U 1 2214 VAh SMX120RMBP2U 2 3690 VAh SMX120RMBP2U 3 5166 VAh SMX120RMBP2U 4 6642 VAh SMX120RMBP2U 6 9594 VAh SMX120RMBP2U 8 12546 VAh SMX120RMBP2U 10 15498 Vah	

IRŚ. 271.1.22.2022

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

na zadanie pn.: *„Dostawa sprzętu i oprogramowania komputerowego w ramach projektu Cyfrowa Gmina z podziałem na części”*

Komunikacja i zarządzanie		
Alarm dźwiękowy	Alarm przy zasilaniu akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia	
Panel przedni	Wyświetlacz statusu led ze wskaźnikiem pracy online: zasilanie akumulatorowe: wskaźniki wymień baterię i przeciążenie Wielofunkcyjna konsola sterownicza i informacyjna lcd	
Awaryjny wyłącznik zasilania	Tak	
Wolne szczeliny	0	
Wstępnie zainstalowane karty SmartSlot™	Network management card 2 with environmental monitoring	
Ochrona przed przepięciami i filtracja		
Znamionowa energia przepięcia (w dżulach)	645 J	
Filtracja	Nieprzerwane filtrowanie zakłóceń na wielu biegunach: przepuszczanie przepięć 0,3% wg ieee: zerowy czas powstrzymywania przepięcia: spełnia wymogi ul 1449	
Jednostka opakowania		
Waga dla opakowania 1	45,36 kg	
Wysokość dla opakowania 1	24,3 cm	
Szerokość dla opakowania 1	59,6 cm	
Ilość jednostek dla opakowania zbiorczego 3	8	
Waga dla opakowania zbiorczego 3	388,69 kg	
Długość dla	100 cm	

opakowania zbiorczego 3		
Ilość warstw na palecie	2	
Warstwy palet	4	
Oferta zrównoważonego rozwoju		
Stan trwałej oferty	Produkt Green Premium	
Rozporządzenie REACh	Deklaracja REACh	
Europejska dyrektywa RoHS	Zgodny Europejska deklaracja RoHS	
Bez rtęci	Tak	
Informacje na temat zwolnienia z RoHS	Tak	
Ujawnienie informacji o wpływie na środowisko	Środowiskowy profil produktu	
Kulistość – profil	Informacja o żywotności	
Optymalna energooszczędność	Product energooszczędny	
Program Take-back	Tak	
Warunki gwarancji		
Gwarancja	3 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulator, możliwość opcjonalnego przedłużenia gwarancji, możliwość dokupienia gwarancji on-site	

1.2. Stacje robocze wraz z monitorami
Ilość: 17 szt.

IRŚ.271.1.22.2022

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

na zadanie pn.: „*Dostawa sprzętu i oprogramowania komputerowego w ramach projektu Cyfrowa Gmina z podziałem na części*"

Parametr	**Charakterystyka (wymagania minimalne)**	**Należy wpisać tak lub nie**
Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.	
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.	
Procesor	Procesor dedykowany do pracy w komputerach stacjonarnych. Procesor osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 20,280 pkt. według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php.	
Pamięć RAM	8GB DDR4 3200MHz. Możliwość rozbudowy do min 64GB, jeden slot DIMM wolny.	
Pamięć masowa	Dysk M.2 SSD 512GB PCIe NVMe Obudowa musi umożliwiać montaż dodatkowego dysku 2.5" lub 3.5"	
Karta graficzna	Zintegrowana z procesorem	
Wyposażenie multimedialne	Karta dźwiękowa min. dwukanałowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo.	
Obudowa	Typu MiniTower z obsługą kart PCI Express wyłącznie o pełnym profilu. Umożliwiająca montaż 1 x dysku 3.5" lub 1 x dysku 2.5" wewnątrz obudowy. Napęd optyczny zamontowany w dedykowanej wnęce zewnętrznej 5.25" typu slim. Obudowa fabrycznie przystosowana do pracy w orientacji pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Suma wymiarów obudowy nieprzekraczająca 800 mm. Zasilacz o mocy min. 180W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Zasilacz w oferowanym komputerze musi się znajdować na stronie http://www.plugloadsolutions.com/80pluspowersupplies.aspx, Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem	

	zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS’u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.	
Bezpieczeństwo	Ukryty w laminacie płyty głównej 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. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność.	
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych	

	odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT” (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. Możliwość dokonywania backup’u BIOS wraz z ustawieniami na dysku wewnętrznym. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS.	
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).	
System operacyjny	Zainstalowany system operacyjny Windows 10 Professional, musi być zapisany trwale w BIOS i umożliwiać reinstalację systemu	

	operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.	
Certyfikaty i standardy	Urządzenia wyprodukowane zgodnie z normą ISO 9001 oraz ISO 50001.	
Wymagania dodatkowe	Wbudowane porty: 1 x HDMI 1.4 1 x DisplayPort 1.4 8 portów USB wyprowadzonych na zewnątrz obudowy, w układzie: Panel przedni: 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0 Panel tylny: 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0 1 x port audio typu combo (słuchawka/mikrofon) na przednim panelu panelu 1 x RJ – 45 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia, wyposażona w: 1 x PCIe x16 Gen.3, 2 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 3 x SATA w tym min. 2 szt SATA 3.0. Jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej. Klawiatura USB w układzie polski programisty Mysz optyczna USB Wbudowana nagrywarka DVD +/-RW o prędkości min. 8x	
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 26 dB	
Wsparcie techniczne producenta	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje,	

	diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).	
Warunki gwarancji	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) 3-letnia gwarancja producenta świadczona na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. W przypadku awarii dysk twardy zostaje u Zamawiającego	
Dodatkowe oprogramowanie	Oprogramowanie producenta komputera z nieograniczoną czasowo licencją na użytkowanie umożliwiające: - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi - dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji - sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania) - dostęp do wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku *.xml	

	Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku. W ofercie należy podać nazwę oprogramowania	
Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą IPS 23,8”	
Rozmiar plamki (maksymalnie)	0,275mm x 0,275mm	
Jasność	250 cd/m2	
Kontrast	Min. 1000:1	
Kąty widzenia (pion/poziom)	178/178 stopni	
Czas reakcji matrycy	Max 8ms (gray to gray)	
Rozdzielczość maksymalna	1920 x 1080 przy 60Hz	
Gama koloru	83% (CIE1976) 72% (CIE1931)	
Pochylenie monitora	W zakresie min. 26 stopni	
Regulacja wysokości	W zakresie 100mm	
Powłoka powierzchni ekranu	Antyodblaskowa	
Podświetlenie	System podświetlenia LED	
Zużycie energii	Maksymalnie 28W, czuwanie maksymalnie 0,3W	
Bezpieczeństwo	Monitor musi być wyposażony dedykowany slot na linkę zabezpieczającą	
Złącza	1x VGA, Display Port 1.2	
Gwarancja	3-letnia gwarancja świadczona na miejscu u klienta. Czas reakcji - do końca następnego dnia roboczego. Wymagane jest oświadczenie Wykonawcy wraz z dostawą sprzętu potwierdzające, że serwis będzie realizowany przez Producenta lub autoryzowanego partnera serwisowego producenta. Monitor musi się znajdować na stronie TCO : http://tcocertified.com/product-finder/	
Inne	VESA 100mm	

1.3. Rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS).
Urządzenie typu firewall spełniające następujące funkcjonalności:

Charakterystyka (wymagania minimalne)	**Należy wpisać tak lub nie**

Samodzielne, dedykowane fizyczne urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej rozwiązania musi występować moduł zarządzania i moduł przetwarzania danych.	
Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.	
Dedykowany port zarządzania out-of-band.	
Brak ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.	
Realizacja zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.	
Obsługa dla IPv6.	
Funkcjonalność statycznej i dynamicznej translacji adresów NAT między IPv4 i IPv6.	
Tworzenie reguł zabezpieczeń firewall zgodnie z ustaloną polityką opartą o profile oraz obiekty.	
Polityka zabezpieczeń firewall musi uwzględniać przynajmniej takie parametry jak: adresy IP źródłowe i docelowe, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie.	
Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.	
Firewall musi działać w następujących trybach: routera (tzn. w warstwie 3 modelu OSI), przełącznika (w warstwie 2 modelu OSI), transparentnym pasywnego nasłuchu.	
Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych biorących udział w transmisji.	
Zarządzanie firewallem musi odbywać się z linii poleceń (CLI) oraz z graficznej konsoli GUI. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Dopuszcza się, aby polityki mogły być tworzone tylko z graficznej konsoli GUI.	
Musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP, mapowanie 1 adres publiczny na 1 adres prywatny oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.+	
Musi umożliwiać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Urządzenia muszą umożliwiać stworzenie co	

najmniej 6 klas dla różnego rodzaju ruchu sieciowego.	
Firewall musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.	
Obsługa protokołu Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.	
Obsługa protokołów routingu dynamicznego, nie mniej niż RIP, OSPF oraz BGP.	
Firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.	
Musi posiadać osobny zestaw polityk definiujący ruch zaszyfrowany SSL oraz SSH, który należy poddać lub wykluczyć z operacji deszyfrowania rozdzielny od polityk bezpieczeństwa.	
Musi posiadać funkcjonalność automatycznego pobierania listy stron WWW lub adresów IP z zewnętrznego systemu oraz używania ich w politykach bezpieczeństwa.	
Ochrona przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony informującej użytkownika o próbie pobrania pliku i możliwości kontynuowania lub zaniechania pobrania.	
Urządzenie zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.	
Firewall musi identyfikować co najmniej 2500 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS m.in.: Skype, Tor, BitTorrent, eMule.	
Możliwość definiowania własnych wzorców aplikacji poprzez zaimplementowane mechanizmy lub z wykorzystaniem serwisu producenta.	
System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie wyłącznie na podstawie rozszerzenia.	
Urządzenie musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Urządzenie musi umożliwiać konfigurację tuneli VPN w trybie route-based VPN.	
Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN oraz IPSec.	
Firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do	

Internetu poza siecią korporacyjną).	
Producent urządzenia musi udostępniać dedykowanego klienta binarnego VPN dla platform Windows, Mac oraz Android.	
Urządzenie musi transparentnie ustalać tożsamość użytkowników sieci w oparciu o Active Directory oraz Ms Exchange. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym Citrix oraz Windows Terminal Services, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.	
Musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach.	
Urządzenie musi obsługiwać nie mniej niż 3 wirtualne routery posiadające odrębne tabele routingu.	
Rozwiązanie musi umożliwiać rozbudowę o możliwość wykrywania domen DGA i ruchu tunelowanego przez DNS. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 36 miesięcy.	
Musi mieć możliwość czytania oryginalnych adresów IP stacji końcowych z nagłówka X-Forwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesje w przypadku gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.	
Musi mieć możliwość wyboru sposobu blokowania ruchu w politykach bezpieczeństwa. Musi istnieć możliwość ustawienia cichego blokowania ruchu bez wysyłania RST, blokowanie z wysłaniem RST tylko do klienta, blokowanie z wysłaniem RST tylko do serwera, blokowanie z wysłaniem RST do klienta i serwera jednocześnie.	
Firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.	
Musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i kategorii stron WWW.	
Urządzenie musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.	
Urządzenie musi być dostarczone w konfiguracji z minimum 8 portami Ethernet 1Gb/s	
Firewall musi posiadać przepustowość w ruchu nie mniej niż 1,8 Gbps dla kontroli firewall z włączoną funkcją kontroli aplikacji. Przepustowość dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (ochrona IPS, antywirus, antyspyware, identyfikacja aplikacji) nie może być mniejsza niż 900 Mbps.	
Urządzenie musi obsłużyć minimum 200 000 jednoczesnych sesji oraz 38 000 nowych połączeń na sekundę.	
Urządzenie musi zapewniać wydajność przynajmniej 1,5 Gbps dla ruchu IPSec VPN i umożliwiać zestawienie przynajmniej 2500 równoczesnych tuneli site-to-site.	

IRŚ.271.1.22.2022

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

na zadanie pn.: *„Dostawa sprzętu i oprogramowania komputerowego w ramach projektu Cyfrowa Gmina z podziałem na części”*

Urządzenie musi być w obudowie typu rack 1RU.	
Urządzenie musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi umożliwiać deszyfracje niezaufanego ruchu HTTPS i poddania go dalszej inspekcji.	
Musi umożliwiać wykluczenie z inspekcji komunikacji szyfrowanej ruchu wrażliwego na bazie co najmniej: kategoryzacji stron URL oraz dodania własnych wyjątków.	
Musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (IPS, AV, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AM, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.	
Urządzenie musi zapewniać zestawienie przynajmniej 1000 sesji SSL VPN.	
Urządzenie musi posiadać funkcjonalność weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci lub wybranych jej zasobów. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania.	
Firewall musi posiadać funkcjonalność sterowania zachowaniem binarnego klienta VPN z poziomu systemu - połączenie automatyczne bądź ręczne przez użytkownika a także umożliwiać sprawdzenie czy klient posiada zainstalowane oprogramowanie antywirusowe. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania.	
Urządzenie musi posiadać funkcjonalność zestawienia tuneli VPN SSL bez konieczności instalowania klienta na stacji końcowej – clientless VPN. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania.	
Musi posiadać możliwość uruchomienia funkcji wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS). W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 12 miesięcy.	
Urządzenie musi posiadać możliwość uruchomienia funkcji inspekcji antywirusowej, kontrolującej przynajmniej protokoły: SMTP, HTTP, POP3, IMAP oraz podstawowe rodzaje plików. Baza AV musi być przechowywana na urządzeniu i regularnie aktualizowana w sposób automatyczny. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 12 miesięcy.	
Firewall musi umożliwiać filtrowanie stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza przypisania URL do kategorii musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 12 miesięcy.	

Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.	
Firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 12 miesięcy.	
Urządzenie musi zapewniać moduł przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box” plików (przynajmniej exe, dll, pdf, jar, apk, pliki MS Office, ELF, BAT, JS, VBS, PS1, shell script, HTA, linki w wiadomościach e-mail) przechodzących przez firewall w celu ochrony przed zagrożeniami typu zero-day. Informacja zwrotna na temat wykrytego złośliwego oprogramowania musi zostać dostarczona na firewall w czasie nie dłuższym jak 5 minut. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików. Jeżeli funkcjonalność wymaga wykupienia dodatkowej licencji wtedy Zamawiający wymaga jej dostarczenia na okres 12 miesięcy.	
Musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive i Active-Active w przypadku pracy z drugim takim samym urządzeniem posiadającym taki sam zestaw licencji.	
Urządzenie musi być rozwiązaniem o uznanej na rynku pozycji i musi znajdować się w kwadracie „Leaders” raportu Gartnera pt. „Magic Quadrant of Network Enterprise Firewalls” w raportach opublikowanych w przeciągu 2 ostatnich lat.	
Urządzenie musi być fabrycznie nowe, aktualnie obecne w linii produktowej producenta.	
Musi pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej.	
Urządzenie nie może znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.	
Serwis dostępu do najnowszej wersji oprogramowania, serwis sprzętowy i ewentualne licencje/subskrypcje na aktualizacje bazy aplikacji muszą być ważne przynajmniej przez okres minimum 12 miesięcy.	
Gwarancja na urządzenie powinna obejmować okres 12 miesięcy.	
Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim.	

1.4. Oprogramowania do tworzenia kopii zapasowych
Obsługujące min. 25 urządzeń w sieci

Charakterystyka (wymagania minimalne)	**Należy wpisać tak lub nie**

IRŚ.271.1.22.2022

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

na zadanie pn.: „*Dostawa sprzętu i oprogramowania komputerowego w ramach projektu Cyfrowa Gmina z podziałem na części*”

Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,	
Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej	
Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.	
Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.	
Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.	
Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej	
Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków	
Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)	
Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji	
Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.	
Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania	
Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.	

Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji	
Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji	
Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)	
Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.	
Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej	
Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.	
Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora	
Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.	
Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)	
Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.	
Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability)	
Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.	
Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik	
Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)	
Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)	

Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.	
Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)	
Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami	
Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre	
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków	
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.	
Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików	
Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.	
Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików: Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs BSD: UFS, UFS2 Solaris: ZFS, UFS Mac: HFS, HFS+ Windows: NTFS, FAT, FAT32, ReFS Novell OES: NSS	
Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.	

Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.	
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),	
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych	
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych	
Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN	
Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.	

1.5. Usługa informatyczna w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania
Ilość: 1 szt.

Zamawiający wymaga, aby wszystkie dostarczone urządzenia zostały umieszczone (zamontowane) i uruchomione we wskazanych przez Zamawiającego miejscach przeznaczenia, w uzgodnionym przez obie strony terminie. Sposób montażu sprzętu ma być dostosowany do technologii wykonania oraz ma być przeprowadzony zgonie z zaleceniami producenta.

Wsparcie techniczne musi być świadczone w języku polskim przez producenta lub oficjalnego partnera producenta urządzeń w zakresie świadczenia pomocy serwisowej.
Wsparcie techniczne musi być świadczone przez okres 12 miesięcy . W ramach świadczenia gwarancyjnego, w wypadku wystąpienia awarii zamawiający otrzyma część zamienną/urządzenie objęte gwarancją w trybie następnego dnia roboczego. Wraz z dostarczonym sprzętem będzie świadczony dostęp do strony pomocy technicznej producenta oraz możliwość pobierania aktualizacji oprogramowania związanego z oferowanym sprzętem.

IRŚ.271.1.22.2022

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

na zadanie pn.: *„Dostawa sprzętu i oprogramowania komputerowego w ramach projektu Cyfrowa Gmina z podziałem na części”*

2) załącznik nr 1b), który otrzymuje brzmienie:

Załącznik nr 1b do SWZ
Informacja o parametrach oferowanego przedmiotu zamówienia Część II

1. serwer

Ilość: 1 szt

Parametr	**Charakterystyka (wymagania minimalne)**	**Należy wpisać tak lub**
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji do 8 dysków 2.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa z możliwością wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.	
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.	
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych	
Procesor	Zainstalowany jeden procesor 16-rdzeniowy, min. 2.4 GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 231 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org w konfiguracji dla dwóch procesorów.	
RAM	64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.	
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing	
Gniazda PCI	- minimum jeden slot PCIe x16 generacji 4	
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)	
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane 3 dyski SSD SATA o pojemności min. 1.92TB, 6Gb, 2,5“ Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.	

	Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde	
Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 4GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED.	
System operacyjny/dodatkowe oprogramowanie	Windows Server 2022 Standard 1x nośnik do downgrade-u do wersji Windows Server 2019 Standard 50x licencja Windows Server 2022/2019 User CALs 1x Microsoft SQL Server 2019 Standard, OEM, Includes 5 Device CALs	
Wbudowane porty	Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,	
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900	
Wentylatory	Redundantne	
Zasilacze	Redundantne, Hot-Plug maksymalnie 800W.	
Bezpieczeństwo	• Zatrzask górnej pokrywy • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem	
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.	
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;	

	• możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera	
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.	
Warunki gwarancji	**3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.** **Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.** **Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń** **Możliwość rozszerzenia gwarancji przez producenta do 7 lat.** **Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera**	
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz	

	warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.	

2. macierz dyskowa
Ilość - 1 szt

Parametr	**Charakterystyka (wymagania minimalne)**	**Należy wpisać tak lub nie**
Procesor	Czterordzeniowy processor AnnapurnaLabs Alpine AL324 ARM Cortex-A57 1,7GHz, 64-bitowy lub o nie gorszych parametrach	
Obudowa	Rack 2U o wymiarach maksymalnych 90(H) x 490(W) x 540(D) mm, wraz z kompletem szyn teleskopowych	
Ilość slotów RAM	1x Long-DIMM DDR4	
Pamięć RAM	4GB UDIMM DDR4, z możliwością rozbudowy do 16GB	
Pamięć Flash	512 MB	
Ilość obsługiwanych dysków	8 dysków 2.5"/3.5" SATA Hot Swap o maksymalnej pojemności 18TB każdy	
Interfejsy sieciowe	2 x Port 2,5 Gigabit (2,5G/1G/100M), 2 x 10 GbE SFP+	
Porty	4x USB 3.2 Gen 1, 1 x PCIe Gen 2 x2	
Wskaźniki LED	HDD 1-8, stan, LAN, Power, USB	
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0,1,5,5+Spare,6,6+Spare,10,10+Spare,50/60.	
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online. Przywracanie RAID.	
Szyfrowanie	Możliwość szyfrowania folderów współdzielonych oraz całych woluminów kluczem AES 256 bitów. Mechanizm szyfrowania z akceleracją sprzętową.	
System Operacyjny	Windows 7, Windows 8, Windows 10, Windows Server 2008R2/2012/2012R2/2016/2019, Apple Mac OS 10.10+, Linux & UNIX	
Zamontowne dyski	4 dyski spełniające poniższe zapisy: Pojemność: minimum 8TB Interfejs: SATA 6Gb/s Pamięć podręczna: 64	

	Prędkość obrotowa: min. 7000 obr/min Gwarancja producenta: 36 miesięcy Usługa odzyskiwania danych świadczona przez producenta dysków.	
Stacja monitoringu	Obsługa do 16 kamer IP (8 darmowych [QVR PRO]).	
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP	
Usługi	Serwer pocztowy, Stacja monitoringu, Windows ACL, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Replikacja w czasie rzeczywistym, Klient LDAP, Serwer Syslog, Migawki wolumenów, Obsługa kontenerów (LXC – Docker), Serwer VPN	
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów	
Rozszerzenie	Możliwość rozszerzenia o maksymalnie 16 zatok	
Gwarancja	Gwarancja 36 miesiące	
Waga	Netto: max 10 kg, Brutto: max 16 kg	
Pobór mocy	Maksymalnie 57 W	
System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+ oraz exFAT	
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation	
Liczba kont użytkowników	4096	
Liczba grup	512	
Liczba udziałów	512	
Max ilość połączeń	700	
Zasilanie	250 W PSU, 100–240 V	
Wentylatory	Minimum 2, o wymiarach co najmniej 70mm	

UPS	Obsługa sieciowych awaryjnych zasilaczy UPS	

3) załącznik nr 7a), który otrzymuje brzmienie:

Załącznik nr 7a do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Część I zakup i dostawa w ramach wydatków bieżących:

- urządzeń podtrzymujących napięcia serwer – UPS,
- stacji roboczych wraz z monitorami,
- oprogramowania do tworzenia kopii zapasowych,
- usług informatycznych w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania,
- rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS).

1. Przedmiot zamówienia obejmuje dostawę następującego sprzętu o parametrach nie gorszych niż wskazane poniżej:

1.1. Zakup urządzenia podtrzymującego napięcie serwera – UPS

Ilość: 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Główne napięcie wejściowe	208 V, 230 V
Inne napięcie wejściowe	220 V, 240 V
Główne napięcie wyjściowe	230 V
Inne napięcie wyjściowe	208 V, 220 V, 240 V
Moc znamionowa w W	2700 W
Moc znamionowa w VA	3000 VA
Typ podłączenia wejściowego	BS1363A Brytyjski, IEC 320 C20, Schuko CEE 7 / EU1-16P
Liczba gniazd zasilających	8 IEC 320 C13, 2 IEC Jumpers, 1 IEC 320 C19
Liczba szaf rackowych	2U
Długość kabla	2,44 m
Liczba kabli	1
Rodzaj akumulatora	Akumulator kwasowo-ołowiowy
Dostarczane wyposażenie	CD z oprogramowaniem, Wsporniki montażowe do szaf przemysłowych Kabel do sygnalizacji RS-232 do Smart-UPS Czujnik temperatury,

	podręcznik użytkownika, Karta do zdalnego zarządzania Web SNMP Management Card
Ogólny	
Number of power module	2400
Liczba slotów wypełnionych modułami mocy	0
Liczba pustych slotów na moduły mocy	0
Product web sub-family	Network card pre-installed
Nadmiarowość	No
Parametry fizyczne	
Kolor	Czarny
Wysokość	8,5 cm
Szerokość	43,2 cm
Głębokość	66,7 cm
Masa produktu	37,32 kg
Miejsce montażu	Przednie
Sposób montażu	W szafie rackowej
Możliwość montażu na dwóch słupkach	0
Kompatybilność z USB	Tak
Na wejściu	
Ograniczenie napięcia wejściowego	140...280 V
Częstotliwość sieciowa	50/60 Hz +/- 3 Hz auto-sensing
Na wyjściu	
Zniekształcenia harmoniczne	Poniżej 5 %
Maksymalna możliwa do konfiguracji moc (w VA)	3000 VA
Maksymalna możliwa do konfiguracji moc (w watach)	2700 W

IRŚ.271.1.22.2022

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

na zadanie pn.: *„Dostawa sprzętu i oprogramowania komputerowego w ramach projektu Cyfrowa Gmina z podziałem na części”*

Czas przełączenia zasilania	2-4 ms, Zazwyczaj 6 ms, maksymalnie 10 ms
Topologia	Line interactive
Typ przebiegu	Sinusoida
Częstotliwość wyjściowa	50/60 Hz +/- 3 Hz synchronicznie z siecią
Certyfikaty i zgodność z normami	
Certyfikaty produktu	C-Tick CE EAC GOST IRAM VDE
Parametry środowiskowe	
Poziom dźwięku	55 dBA
Rozpraszanie ciepła	184 Btu/h
Temperatura otoczenia dla pracy urządzenia	0...40°C
Temperatura otoczenia dla przechowywania	15...45°C
Wilgotność względna	0…95 %
Wilgotność względna (przechowywanie)	0…95 %
Akumulatory i czas podtrzymania	
Rozszerzalny czas podtrzymania	1
Wstępnie zainstalowane baterie	0
Puste gniazda akumulatorowe	0
Typowy czas pełnego ładowania akumulatora	3 godz.
Ilość zestawów RBC™	1
Żywotność akumulatora	min.3 lata
Moc baterii w VAH	738 VAh runtime
Moc akumulatora (W)	245 W rated
Opcja baterii	SMX120RMBP2U 1 2214 VAh SMX120RMBP2U 2 3690 VAh SMX120RMBP2U 3 5166 VAh SMX120RMBP2U 4 6642 VAh SMX120RMBP2U 6 9594 VAh SMX120RMBP2U 8 12546 VAh

	SMX120RMBP2U 10 15498 Vah
Komunikacja i zarządzanie	
Alarm dźwiękowy	Alarm przy zasilaniu akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia
Panel przedni	Wyświetlacz statusu led ze wskaźnikiem pracy online: zasilanie akumulatorowe: wskaźniki wymień baterię i przeciążenie Wielofunkcyjna konsola sterownicza i informacyjna lcd
Awaryjny wyłącznik zasilania	Tak
Wolne szczeliny	0
Wstępnie zainstalowane karty SmartSlot™	Network management card 2 with environmental monitoring
Ochrona przed przepięciami i filtracja	
Znamionowa energia przepięcia (w dżulach)	645 J
Filtracja	Nieprzerwane filtrowanie zakłóceń na wielu biegunach: przepuszczanie przepięć 0,3% wg ieee: zerowy czas powstrzymywania przepięcia: spełnia wymogi ul 1449
Jednostka opakowania	
Waga dla opakowania 1	45,36 kg
Wysokość dla opakowania 1	24,3 cm
Szerokość dla opakowania 1	59,6 cm
Ilość jednostek dla opakowania zbiorczego 3	8
Waga dla opakowania zbiorczego 3	388,69 kg
Długość dla opakowania zbiorczego 3	100 cm
Ilość warstw na palecie	2
Warstwy palet	4
Oferta zrównoważonego rozwoju	
Stan trwałej oferty	Produkt Green Premium

Rozporządzenie REACh	Deklaracja REACh
Europejska dyrektywa RoHS	Zgodny Europejska deklaracja RoHS
Bez rtęci	Tak
Informacje na temat zwolnienia z RoHS	Tak
Ujawnienie informacji o wpływie na środowisko	Środowiskowy profil produktu
Kulistość – profil	Informacja o żywotności
Optymalna energooszczędność	Product energooszczędny
Program Take-back	Tak
Warunki gwarancji	
Gwarancja	3 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulator, możliwość opcjonalnego przedłużenia gwarancji, możliwość dokupienia gwarancji on-site

1.2. Stacje robocze wraz z monitorami
Ilość: 17 szt.

Parametr	Charakterystyka (wymagania minimalne)
Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
Procesor	Procesor dedykowany do pracy w komputerach stacjonarnych. Procesor osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 20,280 pkt. według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php.
Pamięć RAM	8GB DDR4 3200MHz. Możliwość rozbudowy do min 64GB, jeden slot DIMM wolny.
Pamięć masowa	Dysk M.2 SSD 512GB PCIe NVMe Obudowa musi umożliwiać montaż dodatkowego dysku 2.5” lub 3.5”
Karta graficzna	Zintegrowana z procesorem
Wyposażenie multimedialne	Karta dźwiękowa min. dwukanałowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo.
Obudowa	Typu MiniTower z obsługą kart PCI Express wyłącznie o pełnym profilu. Umożliwiająca montaż 1 x dysku 3.5” lub 1 x dysku 2.5” wewnątrz obudowy. Napęd optyczny zamontowany w dedykowanej wnęce zewnętrznej 5.25” typu slim. Obudowa fabrycznie przystosowana do pracy w orientacji pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Suma wymiarów obudowy nieprzekraczająca 800 mm. Zasilacz o mocy min. 180W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Zasilacz w oferowanym komputerze musi się znajdować na stronie http://www.plugloadsolutions.com/80pluspowersupplies.aspx, Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta

	na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS'u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
Bezpieczeństwo	Ukryty w laminacie płyty głównej 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. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność.
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej,

	zintegrowanym układzie graficznym, kontrolerze audio. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT" (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. Możliwość dokonywania backup'u BIOS wraz z ustawieniami na dysku wewnętrznym. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot'owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS.
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
System operacyjny	Zainstalowany system operacyjny Windows 10 Professional, musi być zapisany trwale w BIOS i umożliwiać reinstalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.
Certyfikaty i standardy	Urządzenia wyprodukowane zgodnie z normą ISO 9001 oraz ISO 50001.
Wymagania dodatkowe	Wbudowane porty: 1 x HDMI 1.4 1 x DisplayPort 1.4 8 portów USB wyprowadzonych na zewnątrz obudowy, w układzie: Panel przedni: 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0 Panel tylny: 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0 1 x port audio typu combo (słuchawka/mikrofon) na przednim panelu panelu 1 x RJ – 45 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera)

	wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia, wyposażona w: 1 x PCIe x16 Gen.3, 2 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 3 x SATA w tym min. 2 szt SATA 3.0. Jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej. Klawiatura USB w układzie polski programisty Mysz optyczna USB Wbudowana nagrywarka DVD +/-RW o prędkości min. 8x
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie 26 dB .
Wsparcie techniczne producenta	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).
Warunki gwarancji	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego) 3-letnia gwarancja producenta świadczona na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. W przypadku awarii dysk twardy zostaje u Zamawiającego
Dodatkowe	Oprogramowanie producenta komputera z nieograniczoną czasowo

oprogramowanie	licencją na użytkowanie umożliwiające: - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi - dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne - włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji - sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania) - dostęp do wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml - dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku *.xml Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku. W ofercie należy podać nazwę oprogramowania
Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą IPS 23,8"
Rozmiar plamki (maksymalnie)	0,275mm x 0,275mm
Jasność	250 cd/m2
Kontrast	Min. 1000:1
Kąty widzenia (pion/poziom)	178/178 stopni
Czas reakcji matrycy	Max 8ms (gray to gray)
Rozdzielczość maksymalna	1920 x 1080 przy 60Hz
Gama koloru	83% (CIE1976) 72% (CIE1931)
Pochylenie monitora	W zakresie min. 26 stopni
Regulacja wysokości	W zakresie 100mm
Powłoka powierzchni	Antyodblaskowa

ekranu	
Podświetlenie	System podświetlenia LED
Zużycie energii	Maksymalnie 28W, czuwanie maksymalnie 0,3W
Bezpieczeństwo	Monitor musi być wyposażony dedykowany slot na linkę zabezpieczającą
Złącza	1x VGA, Display Port 1.2
Gwarancja	3-letnia gwarancja świadczona na miejscu u klienta. Czas reakcji - do końca następnego dnia roboczego. Wymagane jest oświadczenie Wykonawcy wraz z dostawą sprzętu potwierdzające, że serwis będzie realizowany przez Producenta lub autoryzowanego partnera serwisowego producenta. Monitor musi się znajdować na stronie TCO : http://tcocertified.com/product-finder/
Inne	VESA 100mm

1.3. Rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS).
Urządzenie typu firewall spełniające następujące funkcjonalności:

Charakterystyka (wymagania minimalne)
Samodzielne, dedykowane fizyczne urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej rozwiązania musi występować moduł zarządzania i moduł przetwarzania danych.
Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
Dedykowany port zarządzania out-of-band.
Brak ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
Realizacja zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.
Obsługa dla IPv6.
Funkcjonalność statycznej i dynamicznej translacji adresów NAT między IPv4 i IPv6.
Tworzenie reguł zabezpieczeń firewall zgodnie z ustaloną polityką opartą o profile oraz obiekty.
Polityka zabezpieczeń firewall musi uwzględniać przynajmniej takie parametry jak: adresy IP źródłowe i docelowe, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie.
Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.
Firewall musi działać w następujących trybach: routera (tzn. w warstwie 3 modelu OSI), przełącznika (w warstwie 2 modelu OSI), transparentnym pasywnego nasłuchu.
Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych biorących udział w transmisji.
Zarządzanie firewallem musi odbywać się z linii poleceń (CLI) oraz z graficznej konsoli GUI. Dostęp do

urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Dopuszcza się, aby polityki mogły być tworzone tylko z graficznej konsoli GUI.
Musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP, mapowanie 1 adres publiczny na 1 adres prywatny oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.+
Musi umożliwiać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Urządzenia muszą umożliwiać stworzenie co najmniej 6 klas dla różnego rodzaju ruchu sieciowego.
Firewall musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
Obsługa protokołu Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.
Obsługa protokołów routingu dynamicznego, nie mniej niż RIP, OSPF oraz BGP.
Firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
Musi posiadać osobny zestaw polityk definiujący ruch zaszyfrowany SSL oraz SSH, który należy poddać lub wykluczyć z operacji deszyfrowania rozdzielny od polityk bezpieczeństwa.
Musi posiadać funkcjonalność automatycznego pobierania listy stron WWW lub adresów IP z zewnętrznego systemu oraz używania ich w politykach bezpieczeństwa.
Ochrona przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony informującej użytkownika o próbie pobrania pliku i możliwości kontynuowania lub zaniechania pobrania.
Urządzenie zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
Firewall musi identyfikować co najmniej 2500 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS m.in.: Skype, Tor, BitTorrent, eMule.
Możliwość definiowania własnych wzorców aplikacji poprzez zaimplementowane mechanizmy lub z wykorzystaniem serwisu producenta.
System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie wyłącznie na podstawie rozszerzenia.
Urządzenie musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Urządzenie musi umożliwiać konfigurację tuneli VPN w trybie route-based VPN.
Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN oraz IPSec.
Firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy

w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną).
Producent urządzenia musi udostępniać dedykowanego klienta binarnego VPN dla platform Windows, Mac oraz Android.
Urządzenie musi transparentnie ustalać tożsamość użytkowników sieci w oparciu o Active Directory oraz Ms Exchange. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym Citrix oraz Windows Terminal Services, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
Musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach.
Urządzenie musi obsługiwać nie mniej niż 3 wirtualne routery posiadające odrębne tabele routingu.
Rozwiązanie musi umożliwiać rozbudowę o możliwość wykrywania domen DGA i ruchu tunelowanego przez DNS. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 36 miesięcy.
Musi mieć możliwość czytania oryginalnych adresów IP stacji końcowych z nagłówka X-Forwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesje w przypadku gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.
Musi mieć możliwość wyboru sposobu blokowania ruchu w politykach bezpieczeństwa. Musi istnieć możliwość ustawienia cichego blokowania ruchu bez wysyłania RST, blokowanie z wysłaniem RST tylko do klienta, blokowanie z wysłaniem RST tylko do serwera, blokowanie z wysłaniem RST do klienta i serwera jednocześnie.
Firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
Musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i kategorii stron WWW.
Urządzenie musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
Urządzenie musi być dostarczone w konfiguracji z minimum 8 portami Ethernet 1Gb/s
Firewall musi posiadać przepustowość w ruchu nie mniej niż 1,8 Gbps dla kontroli firewall z włączoną funkcją kontroli aplikacji. Przepustowość dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (ochrona IPS, antywirus, antyspyware, identyfikacja aplikacji) nie może być mniejsza niż 900 Mbps.
Urządzenie musi obsłużyć minimum 200 000 jednoczesnych sesji oraz 38 000 nowych połączeń na sekundę.
Urządzenie musi zapewniać wydajność przynajmniej 1,5 Gbps dla ruchu IPSec VPN i umożliwiać zestawienie przynajmniej 2500 równoczesnych tuneli site-to-site.
Urządzenie musi być w obudowie typu rack 1RU.
Urządzenie musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi umożliwiać deszyfracje niezaufanego ruchu HTTPS i poddania go dalszej inspekcji.
Musi umożliwiać wykluczenie z inspekcji komunikacji szyfrowanej ruchu wrażliwego na bazie co

najmniej: kategoryzacji stron URL oraz dodania własnych wyjątków.
Musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (IPS, AV, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AM, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
Urządzenie musi zapewniać zestawienie przynajmniej 1000 sesji SSL VPN.
Urządzenie musi posiadać funkcjonalność weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci lub wybranych jej zasobów. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania.
Firewall musi posiadać funkcjonalność sterowania zachowaniem binarnego klienta VPN z poziomu systemu - połączenie automatyczne bądź ręczne przez użytkownika a także umożliwiać sprawdzenie czy klient posiada zainstalowane oprogramowanie antywirusowe. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania.
Urządzenie musi posiadać funkcjonalność zestawienia tuneli VPN SSL bez konieczności instalowania klienta na stacji końcowej – clientless VPN. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania.
Musi posiadać możliwość uruchomienia funkcji wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS). W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 12 miesięcy.
Urządzenie musi posiadać możliwość uruchomienia funkcji inspekcji antywirusowej, kontrolującej przynajmniej protokoły: SMTP, HTTP, POP3, IMAP oraz podstawowe rodzaje plików. Baza AV musi być przechowywana na urządzeniu i regularnie aktualizowana w sposób automatyczny. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 12 miesięcy.
Firewall musi umożliwiać filtrowanie stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza przypisania URL do kategorii musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 12 miesięcy.
Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
Firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum 12 miesięcy.
Urządzenie musi zapewniać moduł przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box” plików (przynajmniej exe, dll, pdf, jar, apk, pliki MS Office, ELF, BAT, JS, VBS, PS1, shell script, HTA, linki w wiadomościach e-mail) przechodzących przez firewall w celu ochrony przed zagrożeniami typu zero-day. Informacja zwrotna na temat wykrytego złośliwego oprogramowania musi zostać dostarczona na firewall w czasie nie dłuższym jak 5 minut. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików. Jeżeli funkcjonalność wymaga wykupienia dodatkowej licencji wtedy Zamawiający wymaga jej dostarczenia na okres 12 miesięcy.
Musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive i Active-Active w przypadku pracy z drugim takim samym urządzeniem posiadającym taki sam zestaw licencji.

Urządzenie musi być rozwiązaniem o uznanej na rynku pozycji i musi znajdować się w kwadracie „Leaders” raportu Gartnera pt. „Magic Quadrant of Network Enterprise Firewalls” w raportach opublikowanych w przeciągu 2 ostatnich lat.
Urządzenie musi być fabrycznie nowe, aktualnie obecne w linii produktowej producenta.
Musi pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej.
Urządzenie nie może znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.
Serwis dostępu do najnowszej wersji oprogramowania, serwis sprzętowy i ewentualne licencje/subskrypcje na aktualizacje bazy aplikacji muszą być ważne przynajmniej przez okres minimum 12 miesięcy.
Gwarancja na urządzenie powinna obejmować okres 12 miesięcy.
Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim.

1.4. Oprogramowania do tworzenia kopii zapasowych
Obsługujące min. 25 urządzeń w sieci

Charakterystyka (wymagania minimalne)
Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności

wymienionych w tej specyfikacji
Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability)
Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik

Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików: Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs BSD: UFS, UFS2 Solaris: ZFS, UFS Mac: HFS, HFS+ Windows: NTFS, FAT, FAT32, ReFS Novell OES: NSS
Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.

1.5. Usługa informatyczna w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania
Ilość: 1 szt.

Zamawiający wymaga, aby wszystkie dostarczone urządzenia zostały umieszczone (zamontowane) i uruchomione we wskazanych przez Zamawiającego miejscach przeznaczenia, w uzgodnionym przez obie strony terminie. Sposób montażu sprzętu ma być dostosowany do technologii wykonania oraz ma być przeprowadzony zgonie z zaleceniami producenta.

Wsparcie techniczne musi być świadczone w języku polskim przez producenta lub oficjalnego partnera producenta urządzeń w zakresie świadczenia pomocy serwisowej.
Wsparcie techniczne musi być świadczone przez okres 12 miesięcy . W ramach świadczenia gwarancyjnego, w wypadku wystąpienia awarii zamawiający otrzyma część zamienną/urządzenie objęte gwarancją w trybie następnego dnia roboczego. Wraz z dostarczonym sprzętem będzie świadczony dostęp do strony pomocy technicznej producenta oraz możliwość pobierania aktualizacji oprogramowania związanego z oferowanym sprzętem.

4) załącznik nr 7b), który otrzymuje brzmienie:

Załącznik nr 7b do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Część II - ***„Zakup i dostawa w ramach zadania inwestycyjnego pn.: „Zakup sprzętu i oprogramowania w ramach projektu Cyfrowa Gmina”:***

1.serwer

Ilość: 1 szt

Parametr	**Charakterystyka (wymagania minimalne)**
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji do 8 dysków 2.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa z możliwością wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość

	konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowany jeden procesor 16-rdzeniowy, min. 2.4 GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 231 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org w konfiguracji dla dwóch procesorów.
RAM	64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	- minimum jeden slot PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane 3 dyski SSD SATA o pojemności min. 1.92TB, 6Gb, 2,5“ Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde
Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 4GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED.
System operacyjny/dodatkowe oprogramowanie	Windows Server 2022 Standard 1x nośnik do downgrade-u do wersji Windows Server 2019 Standard 50x licencja Windows Server 2022/2019 User CALs 1x Microsoft SQL Server 2019 Standard, OEM, Includes 5 Device CALs
Wbudowane porty	Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug maksymalnie 800W.
Bezpieczeństwo	• Zatrzask górnej pokrywy

	• Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server

	2022.
Warunki gwarancji	**3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.** **Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.** **Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń** **Możliwość rozszerzenia gwarancji przez producenta do 7 lat.** **Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera**
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

2. macierz dyskowa
Ilość - 1 szt

Procesor	Czterordzeniowy processor AnnapurnaLabs Alpine AL324 ARM Cortex-A57 1,7GHz, 64-bitowy lub o nie gorszych parametrach
Obudowa	Rack 2U o wymiarach maksymalnych 90(H) x 490(W) x 540(D) mm, wraz z kompletem szyn teleskopowych
Ilość slotów RAM	1x Long-DIMM DDR4
Pamięć RAM	4GB UDIMM DDR4, z możliwością rozbudowy do 16GB
Pamięć Flash	512 MB
Ilość obsługiwanych dysków	8 dysków 2.5"/3.5" SATA Hot Swap o maksymalnej pojemności 18TB każdy
Interfejsy sieciowe	2 x Port 2,5 Gigabit (2,5G/1G/100M), 2 x 10 GbE SFP+
Porty	4x USB 3.2 Gen 1, 1 x PCIe Gen 2 x2
Wskaźniki LED	HDD 1-8, stan, LAN, Power, USB

Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0,1,5,5+Spare,6,6+Spare,10,10+Spare,50/60.
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online. Przywracanie RAID.
Szyfrowanie	Możliwość szyfrowania folderów współdzielonych oraz całych woluminów kluczem AES 256 bitów. Mechanizm szyfrowania z akceleracją sprzętową.
System Operacyjny	Windows 7, Windows 8, Windows 10, Windows Server 2008R2/2012/2012R2/2016/2019, Apple Mac OS 10.10+, Linux & UNIX
Zamontowne dyski	4 dyski spełniające poniższe zapisy: Pojemność: minimum 8TB Interfejs: SATA 6Gb/s Pamięć podręczna: 64 Prędkość obrotowa: min. 7000 obr/min Gwarancja producenta: 36 miesięcy Usługa odzyskiwania danych świadczona przez producenta dysków.
Stacja monitoringu	Obsługa do 16 kamer IP (8 darmowych [QVR PRO]).
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Serwer pocztowy, Stacja monitoringu, Windows ACL, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Replikacja w czasie rzeczywistym, Klient LDAP, Serwer Syslog, Migawki wolumenów, Obsługa kontenerów (LXC – Docker), Serwer VPN
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów
Rozszerzenie	Możliwość rozszerzenia o maksymalnie 16 zatok
Gwarancja	Gwarancja 36 miesiące
Waga	Netto: max 10 kg, Brutto: max 16 kg
Pobór mocy	Maksymalnie 57 W
System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+ oraz exFAT
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
Liczba kont użytkowników	4096
Liczba grup	512

Liczba udziałów	512
Max ilość połączeń	700
Zasilanie	250 W PSU, 100–240 V
Wentylatory	Minimum 2, o wymiarach co najmniej 70mm
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS

II. W związku z powyższym działając na podstawie art. 286 ust. 3 ustawy Prawo zamówień publicznych (t. j. Dz. U. Z 2022 r., poz. 1710 ze zm.):

1) W Rozdziale 12 pkt 12.1. SWZ zmienia się dotychczasowy zapis i przyjmuje się następującą treść:

„Ofertę należy złożyć poprzez miniPortal do dnia 17.01.2023 r. do godziny 09:00.”.

2) W Rozdziale 12 pkt 12.3. SWZ zmienia się dotychczasowy zapis i przyjmuje się następującą treść:

„Otwarcie ofert rozpocznie się w dniu 17.01.2023 r. o godzinie 10:00”.

3) W Rozdziale 10 pkt 10.1. SWZ zmienia się dotychczasowy zapis i przyjmuje się następującą treść:

„Wykonawca będzie związany ofertą do dnia 15.02.2023 r.”

III. Powyższa informacja została zamieszczona w dniu 12.01.2023 r. na:

1) stronie internetowej http://bip.przedborz.pl/,

2) a/a.

Burmistrz Miasta Przedborza

Wiesława Janosik