**Znak sprawy: ZPU 271.19.2022 Załącznik nr 1 do SWZ**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA (SOPZ)**

Niniejszy dokument stanowi szczegółowy opis przedmiotu zamówienia dotyczący zakupu i dostawy sprzętu komputerowego oraz oprogramowania dla Gminy Opatów w ramach projektu Cyfrowa Gmina

1.W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.

2.W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 30 ust. 1 pkt 2 i ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.

3. Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w SOPZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.

4. Dla jednoznacznej identyfikacji oferowanego sprzętu należy podać co najmniej nazwę producenta, a także nazwę i model oferowanego sprzętu. Zamawiający wymaga również podania faktycznych parametrów sprzętu, w taki sposób, by oceniający byli w stanie stwierdzić, czy zaoferowany sprzęt spełnia wymagania specyfikacji. Przedmiotowe informacje są składane na potwierdzenie, iż oferowane urządzenia spełniają wymagania Zamawiającego.

5. O ile inaczej nie zaznaczono, wszelkie zapisy SOPZ zawierające parametry techniczne należy odczytywać jak parametry minimalne.

6. Dostarczany sprzęt musi być fabrycznie nowy i pochodzić z najnowszych linii produktowych.

7. Dostarczany sprzęt musi mieć okablowanie, zasilacze oraz wszystkie inne komponenty, zapewniające właściwą instalację i użytkowanie (np. przewody zasilające itp. ).

8. Sprzęt musi być dostarczony ze wszystkimi niezbędnymi do działania i zapewnienia wymaganych funkcjonalności bezterminowymi licencjami na używanie tych funkcjonalności.

9. Ofertowany sprzęt musi posiadać Certyfikaty ISO1043, ISO9001, ISO14001,deklaracja producenta sprzętu zgodności z CE lub dokument równoważny.

10. Oferowany sprzęt musi spełniać wymogi dyrektywy WEEE 2002/96/EC z dnia 27 stycznia 2003r. dotyczącej odpadów elektrycznych i elektronicznych.

11. Oferowany sprzęt musi spełniać wymagania dyrektywy 2002/95/EC z dnia 27 stycznia 2003 na temat zakazu użycia niebezpiecznych substancji w wyposażeniu elektrycznym i elektronicznym.

12. Gwarancja na dostarczony sprzęt Zamawiający określa na okres w przedziale od 36 miesięcy(termin minimalny) do 60 miesięcy (termin maksymalny). Długość oferowanego okresu gwarancji stanowi jedno z kryterium oceny i zostało szczegółowo opisane w SWZ.

**Zamówienie obejmuje zakup i dostawę następującego sprzętu komputerowego:**

1. **Stacje robocze – 22 szt.**
2. **Monitory – 22 szt.**
3. **Laptopy – 2 szt.**
4. **Oprogramowanie biurowe MS Office – 5 szt.**
5. **Zasilacz awaryjny UPS – 1 szt.**
6. **Urządzenie UTM – 1 szt.**
7. **Serwer z oprogramowaniem – 1 szt.**
8. **Oprogramowanie do szyfrowania wiadomości email – 1 szt.**

**OPIS WYMAGAŃ:**

**Stacje robocze – 22 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane parametry techniczne komputerów** |
| **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, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 20300 pkt. według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php>.  Posiadający co najmniej 6 rdzeni, 12 wątków.  Wynik testu należy dołączyć do oferty. Wynik nie może być późniejszy niż 30 dni przed złożeniem oferty. |
| **Pamięć RAM** | 16GB DDR4 3200MHz, możliwość rozbudowy do min 64GB, minimum jeden slot DIMM wolny. |
| **Pamięć masowa** | Min. 512GB SSD PCIeNVMe  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 Small Form Factor z obsługą kart wyłącznie o niskim profilu. Umożliwiająca montaż 1 x dysku 3.5” lub 1 x dysku 2.5” wewnątrz obudowy. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Suma wymiarów obudowy nieprzekraczająca 700 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>, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus  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 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) oraz posiadać zamontowany wewnątrz filtr przeciwpyłowy. 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 technologi wirtualizacji realizowane łącznie w procesorze, chipsecie płyty główej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |
| **System operacyjny** | Zainstalowany system operacyjny Windows 11 Professional, musi być zapisany trwale w BIOS i umożliwiać reinstalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.  (lub równoważny w pełni działający w domenie Active Directory Windows Server 2019)  Równoważność – Microsoft  Zamawiający wskazał w niniejszym załączniku znak towarowy firmy Microsoft jako wzorzec funkcjonalno-jakościowy przedmiotu zamówienia.  Oznacza to tym samym, że Zamawiający dopuszcza złożenie oferty zawierającej sprzęt z systemem operacyjnym o parametrach funkcjonalnych i wydajnościowych nie gorszych od parametrów systemu operacyjnego określonego we wzorcu, o ile jednocześnie zostaną zachowane pozostałe wymagania określone w SWZ i zaoferowany system operacyjny będzie w pełni i poprawnie funkcjonował z posiadaną i użytkowaną infrastrukturą informatyczną (sprzęt i oprogramowanie) Zamawiającego, tj. w szczególności z:  • sieciowymi systemami operacyjnymi MS Windows;  • oprogramowaniem aplikacyjnym - MS Office, ESET Antyvirus, WinRAR, Windows Internet Explorer, Adobe Reader, Legislator, Szafir, Korelacja;  • urządzeniami drukującymi-kopiującymi-skanującymi firm HP, Kyocera, Konica Minolta(oficjalnie dostępne sterowniki producentów urządzeń dla oferowanego systemu operacyjnego).  Wykazanie równoważności oferowanych produktów leży po stronie Wykonawcy i powinno zostać przez niego udokumentowane i złożone wraz z ofertą.  W przypadku zaoferowania przez Wykonawcę innego systemu operacyjnego niż MS WINDOWS – dokumenty poświadczające równoważność złożone przez Wykonawcę zostaną przesłane do producenta ww. oprogramowania lub urządzeń, celem jego weryfikacji. |
| **Certyfikaty i standardy** | Deklaracja zgodności CE (załączyć do oferty)  Urządzenia wyprodukowane, zgodnie z normą ISO 9001 oraz ISO 50001 – certyfikaty załączyć do oferty  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram.  Certyfikat Epeat min. Silver dla Polski (załączyć wydruk ze strony <https://www.epeat.net/> ) lub certyfikat TCO (załączyć wydruk ze strony <https://tcocertified.com/> ) dla oferowanego modelu |
| **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, 1 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 2 x SATA w tym min. 1 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 |
| **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 (załączyć oświadczenie producenta). |
| **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 – dokumenty potwierdzające załączyć do oferty.  Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia Producenta potwierdzonego, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta  W przypadku awarii dysk twardy zostaje u Zamawiającego – do oferty załączyć oświadczenie podmiotu realizującego serwis lub producenta o spełnieniu tego warunku |
| **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 |

|  |  |
| --- | --- |
| **Warunki gwarancyjne, wsparcie techniczne** | Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.  Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego)  3-letnia gwarancja producenta świadczona na miejscu u klienta, Czas reakcji serwisu - do końca następnego dnia roboczego.  W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku  Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.  Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia Producenta potwierdzonego, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta |

**Monitory – 22 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane parametry techniczne** |
| **Typ ekranu** | Matryca LED TN min. 21” |
| **Rozmiar plamki (maksymalnie)** | 0,248 x 0,248 mm |
| **Jasność** | Min. 200 cd/m2 |
| **Kontrast** | Min. 600:1 |
| **Kąty widzenia (pion/poziom)** | Min. 170/160 stopni |
| **Czas reakcji matrycy**  **(maksymalnie)** | 5ms (gray to gray) |
| **Rozdzielczość maksymalna** | 1920 x 1080 przy 60Hz |
| **Powłoka powierzchni ekranu** | Antyodblaskowa lub Matowa |
| **Podświetlenie** | System podświetlenia LED |
| **Zużycie energii** | Maksymalne 15W, czuwanie nie więcej niż 0.3W |
| **Bezpieczeństwo** | Monitor musi być wyposażony w dedykowany slot na linkę zabezpieczającą |
| **Złącze** | 1 x 15-stykowe złącze D-Sub,  1 x HDMI 1.4 lub 1 x złącze DisplayPort 1.2 |
| **Gwarancja** | Czas trwania gwarancji min. 3 lata  Czas reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.  Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.  Gwarancja zero martwych pikseli |
| **Certyfikaty** | EPEAT Gold, Energy Star 8.0  Monitor musi się znajdować na stronie TCO:  http://tcocertified.com/product-finder/ |
| **Inne** | Monitor musi posiadać trwałe oznaczenie logo producenta jednostki centralnej. Odłączany stand bez użycia narzędzi  VESA 100mm. |

**MS Office Home and Business 2021 - 5 szt.**

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane parametry** |
| Office Home and Business 2021 | Licencja na program Microsoft Office 2021 Home & Business PL 32/64 lub równoważne spełniające wymagania  Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Musi zawierać co najmniej następujące komponenty:   * edytor tekstu, * arkusz kalkulacyjny, * program do przygotowywania i prowadzenia prezentacji, * program do zarządzania informacją przez użytkownika (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami);   2. Wszystkie komponenty oferowanego pakietu biurowego muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzanie i wymiana danych), posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi;  3. Dostępna pełna polska wersja językowa interfejsu użytkownika, systemu komunikatów i podręcznej kontekstowej  pomocy technicznej;  4. Prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach: doc, docx, xls, xlsx, ppt, pptx, pps, ppsx, w  tym obsługa formatowania bez utraty parametrów i cech użytkowych (zachowane wszelkie formatowanie,  umiejscowienie tekstów, liczb, obrazków, wykresów, odstępy między tymi obiektami i kolorów);  5. Wykonywanie i edycja makr oraz kodu zapisanego w języku Visual Basic w plikach xls, xlsx oraz formuł w plikach  wytworzonych w MS Office 2019, 2021 bez utraty danych oraz bez konieczności przerabiania dokumentów;  6. Możliwość zapisywania wytworzonych dokumentów bezpośrednio w formacie PDF;  7. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową Active Directory;  8. Możliwość nadawania uprawnień do modyfikacji i formatowania dokumentów lub ich elementów;  9. Możliwość jednoczesnej pracy wielu użytkowników na udostępnionym dokumencie arkusza kalkulacyjnego;  10. Posiadać pełną kompatybilność z systemami operacyjnymi:  MS Windows 10, 11 (32 i 64-bit)  Licencja komercyjna, umożliwiająca przenoszenie (deinstalację z jednego komputera i instalację na innym), wraz z zapewnieniem dostępu do zbiorów instalacyjnych. |

**Laptopy – 2 szt.**

|  |  |
| --- | --- |
| **Nazwa** | **Wymagane parametry techniczne** |
| **Zastosowanie** | Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, dostępu do Internetu oraz poczty elektronicznej. |
| **Matryca** | 15.6” FHD (1920 x 1080), powłoka matowa, |
| **Procesor** | Oferowany komputer przenośny musi osiągać w teście wydajności Passmark CPU Mark, w kategorii Average CPU Mark co najmniej 10000 punktów według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php>  Procesor 4 rdzeniowy 8 wątkowy, o TDP typowym 15W I maksymalnym do 40W  Wynik testu procesora należy dołączyć do oferty jako załącznik.  Wynik nie może być późniejszy niż 30 dni przed złożeniem oferty. |
| **Pamięć RAM** | 16GB DDR4, możliwość rozbudowy do min. 64GB, nie dopuszcza się pamięci wlutowanych w płytę główną, min. dwa sloty na pamięć |
| **Pamięć masowa** | 512GB SSD M.2 PCIeNVMe Class 35 |
| **Karta graficzna** | Zintegrowana z procesorem. |
| **Klawiatura** | Klawiatura w układzie US – QWERTY z wydzieloną klawiaturą numeryczną, z wbudowanym podświetleniem, min 90 klawiszy. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, printscreen dostępne w ciągu klawiszy F1-F12. |
| **Multimedia** | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo.  Dwa kierunkowe, cyfrowe mikrofony z funkcją redukcji szumów i poprawy mowy wbudowane w obudowę matrycy.  Kamera internetowa z diodą informującą o aktywności, min. 0.9 Mpix, trwale zainstalowana w obudowie matrycy, czytnik kart micro SD 4.0, 1 port audio typu combo (słuchawki i mikrofon) |
| **Łączność bezprzewodowa** | Karta Wi-Fi AX + Bluetooth 5.2 |
| **Bateria i zasilanie** | Min. 3-cell [min. 40Whr].  Zasilacz o mocy min. 60W |
| **Waga i wymiary** | Waga max 1,8kg z baterią |
| **BIOS** | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji, oraz posiadać: datę produkcji komputera (data produkcji nieusuwalna), o kontrolerze audio, procesorze, a w szczególności min. i max. osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne (nieedytowalne) pole assettag z możliwością wpisywania min. znaków specjalnych. Funkcje logowania się do BIOS na podstawie hasła systemowego/użytkownika, administratora (hasła niezależne), Blokowanie hasłem systemowym/użytkownika rozruch dysku twardego. Funkcja umożliwiająca założenie hasła na dysk, informację o stanie naładowania baterii (stanu użycia), podpiętego zasilacza, zarządzanie trybem ładowania baterii (np. określenie docelowego poziomu naładowania). Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS.  Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym. |
| **Certyfikaty** | Certyfikat ISO9001 dla producenta sprzętu (należy załączyć do oferty)  Certyfikat ISO 14001 dla producenta sprzętu (należy załączyć do oferty)  Certyfikat ISO 50001 dla producenta sprzętu (należy załączyć do oferty)  Certyfikacja TCO dla oferowanego modelu dostępna na stronie <https://tcocertified.com/product-finder/> lub załączyć certyfikat do oferty  Deklaracja zgodności CE (załączyć do oferty)  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki  Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony) |
| **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 23dB (załączyć do oferty oświadczenie producenta potwierdzające spełnienie wymogu) |
| **Diagnostyka** | System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. Działający w pełni, bez okrojonych funkcjonalności nawet w przypadku uszkodzonego dysku, braku dysku lub sformatowanym dysku, dostępu do sieci i internetu oraz bez konieczności podłączenia urządzeń wewnętrznych i zewnętrznych oraz bez konieczności pobierania i instalowania np. na ukrytej pamięci flash BIOS |
| **Bezpieczeństwo** | Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej. |
| **System operacyjny** | Zainstalowany system operacyjny Windows 11 Professional, musi być zapisany trwale w BIOS i umożliwiać reinstalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.  (lub równoważny w pełni działający w domenie Active Directory Windows Server 2019)  Równoważność – Microsoft  Zamawiający wskazał w niniejszym załączniku znak towarowy firmy Microsoft jako wzorzec funkcjonalno-jakościowy przedmiotu zamówienia.  Oznacza to tym samym, że Zamawiający dopuszcza złożenie oferty zawierającej sprzęt z systemem operacyjnym o parametrach funkcjonalnych i wydajnościowych nie gorszych od parametrów systemu operacyjnego określonego we wzorcu, o ile jednocześnie zostaną zachowane pozostałe wymagania określone w SWZ i zaoferowany system operacyjny będzie w pełni i poprawnie funkcjonował z posiadaną i użytkowaną infrastrukturą informatyczną (sprzęt i oprogramowanie) Zamawiającego, tj. w szczególności z:  •sieciowymi systemami operacyjnymi MS Windows;  •oprogramowaniem aplikacyjnym - MS Office, ESET Antyvirus, WinRAR, Windows Internet Explorer, Adobe Reader, Legislator, Szafir, Korelacja;  •urządzeniami drukującymi-kopiującymi-skanującymi firm HP, Kyocera, Konica Minolta (oficjalnie dostępne sterowniki producentów urządzeń dla oferowanego systemu operacyjnego).  Wykazanie równoważności oferowanych produktów leży po stronie Wykonawcy i powinno zostać przez niego udokumentowane i złożone wraz z ofertą.  W przypadku zaoferowania przez Wykonawcę innego systemu operacyjnego niż MS WINDOWS – dokumenty poświadczające równoważność złożone przez Wykonawcę zostaną przesłane do producenta ww. oprogramowania lub urządzeń, celem jego weryfikacji. |
| **Oprogramowanie dodatkowe** | Dołączone do oferowanego komputera oprogramowanie z nieograniczoną licencją czasowo 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,  - możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji:                  a. o poprawkach i usprawnieniach dotyczących aktualizacji                  b. dacie wydania ostatniej aktualizacji                  c. priorytecie aktualizacji                  d. zgodność z systemami operacyjnymi                  e. jakiego komponentu sprzętu dotyczy aktualizacja                  f.  wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.  - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne  - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.  - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr)  - sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania)  - dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml  - raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku \*.xml od razu spakowany z rozszerzeniem \*.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku. |
| **Porty i złącza** | Wbudowane porty i złącza: 1x HDMI 2.0, 2x USB 3.2 typ A, 1x RJ - 45 [fizyczny port], port audio combo |

**Zasilacz awaryjny UPS – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane parametry techniczne** |
| **Moc wyjściowa, pozorna/czynna** | 3000VA/2700W |
| **Liczba faz napięcia (wejście / wyjście)** | 1/1 |
| **Typ obudowy** | RACK |
| **Topologia** | on-line |
| **Środowisko pracy** | Pomieszczenia biurowe / przemysłowe o niskim poziomie zanieczyszczeń |
| **Napięcie znamionowe (wartość skuteczna)** | 230 V AC |
| **Częstotliwość znamionowa napięcia wejściowego** | 50 Hz |
| **Czas przełączenia na pracę rezerwową** | 4 ms |
| **Czas powrotu na pracę sieciową** | 0 ms |
| **Przeciążalność** | > 105% - 15 s (wyłączenie UPS) |
| **Akumulatory wewnętrzne** | 12 V / 9 Ah |
| **Liczba akumulatorów wewnętrznych** | 6 |
| **Napięcie ładowania** | 82 VDC +/- 1% |
| **Maksymalny czas ładowania baterii wewnętrznych UPS do 90%** | 4 h |
| **Zabezpieczenie wejściowe** | Przeciwzwarciowe – Bezpiecznik automatyczny 16 A/ 250 V AC |
| **Przyłącze zasilania UPS** | 1 x IEC 320 C20 (16 A) |
| **Przyłącza wyjściowe (liczba i typ gniazd)** | 1x IEC320 C19 (16A)  8x IEC320 C13 (10A) |
| **Sygnalizacja** | Akustyczno – optyczna; graficzny wyświetlacz LCD, dioda LED |
| **Deklaracje** | CE |
| **Normy** | PN-EN 62040-1:2009, PN-EN 62040-2:2008 |

**Urządzenie UTM – 1 szt.**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

* W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive.
* Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
* Monitoring stanu realizowanych połączeń VPN.
* System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
* System realizujący funkcję Firewall powinien dysponować minimum 10 portami Ethernet 10/100/1000 Base-TX
* System powinien umożliwiać zdefiniowanie co najmniej 250 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
* W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę
* Przepustowość Firewall’a: nie mniej niż 10 Gbps
* Wydajność szyfrowania VPN IPSec: nie mniej niż 6500 Mbps
* System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
* System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń.
* W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:
* Kontrola dostępu - zapora ogniowa klasy StatefulInspection
* Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
* Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN
* Ochrona przed atakami - IntrusionPrevention System
* Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
* Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP
* Kontrola pasma oraz ruchu [QoS, Trafficshaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma
* Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów)
* Możliwość analizy ruchu szyfrowanego protokołem SSL
* Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
* Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) - minimum 1400 Mbps
* Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 700 Mbps
* W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż:
* Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
* Praca w topologii Hub and Spoke oraz Mesh
* Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
* W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
* Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
* Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall’a, IPSecVPN’aAntywirus’a, IPS’a.
* Translacja adresów NAT adresu źródłowego i docelowego.
* Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.
* Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
* Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) ) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR.
* Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
* Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
* Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxyavoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.
* Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
* System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż:
* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
* haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
* haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
* Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory
* Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:
* ICSA lub EAL4 dla funkcji Firewall
* ICSA lub NSS Labs dla funkcji IPS
* ICSA dla funkcji: SSL VPN, IPSec VPN
* Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
* Serwisy i licencje
* W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 3 lat.
* Gwarancja oraz wsparcie

Gwarancja: System powinien być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.

W ramach dostawy do obowiązków Wykonawcy należy:

- montaż, instalacja i prawidłowa konfiguracja UTM ,

- przeprowadzenie instruktarzu dla administratora Zamawiającego.

**Serwer z oprogramowaniem – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane parametry techniczne komputerów** |
| **Obudowa** | RACK 1U Panel przedni chroniący kluczem dostępu do dysków Czujnik otwarcia obudowy |
| **Procesor** | Procesor z obsługą wirtualizacji.Jeden procesor czterordzeniowy z obsługą instrukcji 64 bitowych umożliwiający osiągnięcie wyniku min. 6800 punktów w teście PassMark CPU Benchmarks dostępnym na stronie <http://www.cpubenchmark.net/high_end_cpus.html>.  Wynik testu należy dołączyć do oferty.  Wynik nie może być późniejszy niż 30 dni przed złożeniem oferty. |
| **Pamięć RAM** | min. 16GB dedykowane do pracy serwerowej |
| **Pamięć masowa** | 4 kieszenie HotSwap SATA3 1 dysk systemowy o poj. min. 1TB zamontowany w kieszeni HotSwap 3 dyski na dane o poj. min. 2TB zamontowane w kieszeniach HotSwap. |
| **Obsługa sieci:** | min. 2 karty sieciowe LAN RJ45 10/100/1000 Mb/s |
| **Inne:** | Wsparcie KVM przez LAN Komplet szyn montażowych w zestawie |
| **Gwarancja** | 3 lata gwarancji producenta |

***Oprogramowanie serwera zarządzania komputerami przy pomocy kontrolera domeny, wsparcie techniczne i prawo do aktualizacji na min. 2 lata.***

1. **Oprogramowanie dostarczone razem z serwerem musi zapewnić możliwość zarządzania systemem i konfiguracją przez przeglądarkę WEB, zapewniając funkcjonalność:**
2. interfejs obsługi serwera musi być realizowany przez najnowszą przeglądarkę internetową i być w standardzie Windows METRO,
3. system powinien przed zalogowaniem do panelu zarządzającego informować w czasie rzeczywistym administratora o obciążeniu: całego systemu, procesora, pamięci oraz interfejsu sieciowego na dynamicznych wykresach. Wskazując myszką dane na wykresie powinny pokazywać wartość obciążenia. Informacje o obciążeniu całego systemu, procesora, pamięci oraz interfejsu sieciowego powinny być archiwizowane w serwerze i dostępne przez system raportujący dla okresów: godzinowy, dzienny, tygodniowy i miesięczny,
4. serwer musi umożliwiać realizowanie usług (FTP, FTP z opcją szyfrowania SSL/TLS, TFTP, NFS),
5. musi posiadać system antywirusowy,
6. możliwość zarządzania serwerem poprzez protokół SNMP w wersji 1/2/3,
7. musi umożliwiać dostęp administratorów przez przeglądarkę WEB,
8. wbudowany firewall zarządzany przez przeglądarkę WEB,
9. przed zalogowaniem administratora do interfejsu serwera WEB, powinien bez autoryzacji odczytywać parametry obciążenia serwera pokazywane na dynamicznych wykresach w przeglądarce WEB,
10. system musi umożliwiać generowanie certyfikatów SSL przez przeglądarkę WEB,
11. system powinien posiadać możliwość importowania zewnętrznych certyfikatów SSL przez przeglądarkę WEB,
12. **W zakresie obsługi domeny, dostarczone oprogramowanie musi zapewnić funkcjonalność:**
13. zarządzania do min. 25 użytkowników, grup,
14. zarządzanie do min. 25 komputerów,
15. zarządzanie do min. 25 urządzeń,
16. zarządzania polisami GPO,
17. obsługę profili użytkowników oraz profili mobilnych,
18. obsługę do min. 45 jednoczesnych podłączeń do serwera domeny,
19. zarządzania użytkownikami, grupami, komputerami podpiętymi do kontrolera domenowego przez przeglądarkę WEB,
20. możliwość tworzenia użytkowników i grup w kontrolerze domeny przez przeglądarkę WEB,
21. nadawania haseł dla użytkowników w kontrolerze domeny przez przeglądarkę WEB,
22. wyszukiwania po nazwie użytkownika, grupy i komputera przez przeglądarkę WEB,
23. listy użytkowników, którym wygasła ważność konta dostępna w przeglądarce WEB,
24. listy zablokowanych kont w kontrolerze domeny dostępna w przeglądarce WEB,
25. wszystkie operacje zakładania i modyfikacji oraz usuwania kont, grup, komputerów w kontrolerze domenowym przez przeglądarkę WEB powinny być raportowane w centralnym repozytorium systemowym,
26. możliwość wyświetlenia oraz akceptowania polityki bezpieczeństwa przed zalogowaniem użytkowników do serwera domenowego,
27. administrator podłączający się do kontrolera domeny musi mieć możliwość autoryzacji i logowania się do serwera domenowego przy pomocy jednego dostarczonego do serwera urządzenia sprzętowego token wykorzystujący port USB,
28. Administrator zanim dokona logowania do kontrolera domeny przy pomocy urządzenia sprzętowego token może wyświetlić wewnętrzną politykę bezpieczeństwa informacji Urzędu. Administrator Bezpieczeństwa Informacji ma możliwość zarządzania treścią, która jest wyświetlana i akceptowana w procesie logowania do systemu operacyjnego lub kontrolera domeny.
29. Administrator wyciągając urządzenie autoryzacyjne token z portu USB będzie miał blokowany system operacyjny.
30. Zastosowane urządzenie sprzętowe token powinno umożliwiać przypisywanie konkretnego komputera (wraz z logowaniem administrator do kontrolera domeny) do urządzenia sprzętowego token,
31. Pamięć urządzenia sprzętowego token musi umożliwiać zdefiniowania do 20 uwierzytelnień do systemu operacyjnego i kontrolera domeny,
32. Urządzenie sprzętowe token musi wykorzystywać tylko jeden port USB w wersji 2.0 lub 3.0,
33. Urządzenie sprzętowe token w celu uwierzytelnienia musi wymagać stosowania min. 6 znakowego PIN-u,
34. współpracy z klientami Windows 7,8,8.1,10, 11 w wersji professional.
35. **Licencja kontrolera domeny dla zamawianego serwera głównego musi umożliwiać:**
36. łatwe uruchomienie kontrolera domeny w trybie awaryjnym (w ograniczonej funkcjonalności) na dowolnym serwerze posiadanego przez zamawiającego na czas naprawy zamówionego serwera głównego.
37. **Oprogramowanie musi umożliwiać wirtualizację dowolnych systemów operacyjnych i musi realizować:**
38. obsługę minimum cztero-rdzeniowego procesora,
39. obsługę minimum 32GB RAM-u,
40. obsługę vmware VMDK,
41. obsługę minimum 10 instancji środowisk wirtualnych,
42. zapis stanu maszyny wirtualnej tzw. snapshot,
43. kopii stanu maszyny wirtualnej,
44. emulacji wielu urządzeń np. kart sieciowych, kontrolerów SAS,
45. dynamicznej alokacji pamięci na kontener danych
46. współpracy z kontrolerami SATA, SCSI,
47. tryb pracy sieciowej min NAT, tunel UD, Bridge oraz wielu interfejsów sieci,
48. zarządzanie poprzez przeglądarkę WEB,
49. archiwizacje uruchomionych maszyn wirtualnych.
50. **Oprogramowanie musi również umożliwiać migrację użytkowników lokalnych do serwera domenowego działającego w systemie Windows Vista,7,8,8.1,10, 11 w wersji 32 i 64 bity w wersji professional z licencją na użytkowanie bezterminową umożliwiając przenoszenie do 45 użytkowników i musi realizować:**
51. automatyczne przenoszenie profili i ustawień użytkownika z konta lokalnego do konta domenowego,
52. automatyczne przeniesienie dokumentów użytkownika z konta lokalnego do konta domenowego i nadanie odpowiednich uprawnień ACL,
53. automatyczne przenoszenie uprawnień plikowych i rejestru z konta lokalnego do konta domenowego
54. automatyczne przeniesienie lokalnej skrzynki pocztowej Microsoft Outlook i Thunderbird z domyślnej lokalizacji w koncie lokalnym do konta domenowego.

***Specyfikacja wdrożenia:***

1. **Wykonawca do wdrożenia oferowanych rozwiązań musi posiadać następujące osoby z uprawnieniami:**
2. jedną osobę posiadającą uprawnienia Audytora Wiodącego ISO 27001:2013 i Audytora Wewnętrznego ISO 14001 i 50001 lub uprawnienia równoważne,
3. jedną osobę posiadającą uprawnienia Audytora Wewnętrznego ISO 27001:2013 i MCSA SQL Server 2012 i MCSA Windows Server 2012 lub uprawnienia równoważne.
4. **W ramach wdrożenia wykonawca przeszkoli kadrę informatyczną Urzędu z wdrożonych rozwiązań. Osoba szkoląca musi posiadać uprawnienia Audytora Wiodącego ISO 27001:2013 lub uprawnienia równoważne.**
5. **Wdrożenie i szkolenie z oprogramowania musi być realizowane przez certyfikowanych inżynierów z uprawnieniami wystawionymi przez producenta.**

**Oprogramowania do szyfrowania wiadomości email technologią END TO END, licencja dla min. 25 jednostek komputerowych. Wsparcie techniczne i prawo do aktualizacji na min. 2 lata. Bazy reguł, sygnatur i zagrożeń phishing na min. 2 lata.**

1. **Oprogramowanie musi zapewnić funkcjonalność:**
2. szyfrowanie algorytmem AES256 treści wiadomości,
3. szyfrowanie algorytmem AES256 załączników,
4. szyfrowanie algorytmem AES256 plików,
5. szyfrowanie algorytmem AES256 katalogów,
6. do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagany jest dodatkowy płatny lub bezpłatny dostęp do usług internetowych, chmury, hostingu lub portalu internetowego.
7. do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagane jest połączenie Internetowe.
8. do odszyfrowania wiadomości nie jest potrzebne wysyłanie linków do oprogramowania deszyfrującego.
9. do odszyfrowania treści wiadomości nie jest wymagane instalowanie dodatkowego oprogramowania deszyfrującego.
10. odszyfrowanie treści wiadomości, plików, katalogów, załączników email musi być możliwe na popularnych systemach operacyjnych z środowiskiem graficznym: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11,Ubuntu Desktop 20.04.3 ,Ubuntu Desktop 21.10, Linux Mint 20.2, Fedora Workstation 35, macOS 11, Android od wersji 6.0
11. szyfrowana zawartość wiadomości może zawierać nie tylko tekst ale również elementy graficzne takie jak: HTML, obrazki
12. generowania bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla szyfrowania,
13. opieczętowania każdej wysłanej wiadomość sygnaturą, która jednoznacznie wskazuje na jej oryginalność,
14. zabezpieczenia każdego emaila dedykowanym unikalnym hasłem,
15. posiadania wewnętrznej bazy haseł, która umożliwia:
    1. export haseł do pliku,
    2. import haseł z pliku
    3. generowania ponownie haseł w bazie
16. posiadania wewnętrznego raportu informującego administratora o szyfrowaniu email przy włączonej opcji generowania hasła dla każdej z nich,
17. posiadania wewnętrznego raportu z historią szyfrowanych plików i katalogów wraz z przypisanym hasłem szyfrującym,
18. posiadania menu kontekstowego do szybkiego wybierania szyfrowania wiadomości emailowych, plików i katalogów,
19. pracy i pomocy zdalnej użytkownikom poprzez przejęcie zdalnego pulpitu również poza siecią lokalną z użyciem jednorazowych wygenerowanych kodów autoryzacyjnych. Dodatkowo system pracy zdalnej musi działać niezależnie od włączonej funkcji UAC w systemie Windows.
20. integracji z komórką (Android, IOS, Windows Phone) umożliwiającą wygenerowanie sms-a z hasłem i docelowym kontaktem sms-owym,
21. zabezpieczenia panelu ustawień oprogramowania poprzez hasło dostępowe,
22. wykrywania fałszywych emaili - Antiphishing,
23. wykrywania prób podszycia się pod dowolnego adresata - mechanizm ANTISPOOFING,
24. wykrywania fałszywych linków i odsyłaczy w wiadomościach emailowych,
25. wykrywanie niebezpiecznych dokumentów MS Office,
26. wykrywanie niebezpiecznych rozszerzeń plików przesyłanych przez pocztę email,
27. definiowania alarmów informujących o niebezpiecznych mailach i załącznikach,
28. współpracę z serwerem producenta oprogramowania dostarczającym bazy reguł, sygnatur, zagrożeń phishingowych. Dostęp do tej bazy wymagany jest minimum na 2 lata. Baza reguł, sygnatur i zagrożeń phishingowych powinna posiadać min. 1 500 000 wpisów. Producent musi umożliwiać wyświetlenie ilości wpisów na aktualny dzień poprzez stronę Internetową. Wpisy do bazy muszą być weryfikowane min. 2 razy w ciągu dnia,
29. alarmowanie o wybranych zagrożeniach phishingowych min. raz na miesiąc,
30. współpracy z klientem Mozilla Thunderbird i Mozilla ThunderbirdPortable dla systemów 32 i 64 Bit Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11.
31. **Licencja na użytkowanie oprogramowania musi być wieczysta i nie może być uzależniona oraz powiązana z innym oprogramowaniem do bezpieczeństwa np. antywirusy.**
32. **Oprogramowanie musi działać samodzielnie i do poprawnej jego pracy nie może wymagać innych pakietów bezpieczeństwa np. antywirusy.**
33. **Oprogramowanie musi poprawnie działać z różnymi zainstalowanymi antywirusami.**
34. **Oprogramowanie nie może wyłączać domyślnego antywirusa systemowego Windows.**
35. **Przeprowadzenie cyklicznych zdalnych szkoleń minimum raz w roku z tematyki cyberbezpieczeństwa, zagrożeń poczty email, przepisów prawnych w kontekście normy ISO 27001 przez Audytora Wiodącego ISO 27001 lub uprawnienia równoważne przez 2 lata.**