

ZPI.271.12.2023

Załącznik nr 8 do SWZ

## Opis przedmiotu zamówienia

### „Cyfrowa Gmina”

Przedmiotem zamówienia jest dostawa sprzętu komputerowego wraz z oprogramowaniem zgodnie z poniższym zestawieniem. Sprzęt będzie fabrycznie nowy, nieużywany, sprawny i nie może być przedmiotem praw ani zobowiązań osób trzecich.

#### Stanowiska robocze stacjonarne

Komputer – 5 sztuk

Nazwa komponentu	Wymagane minimalne 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. Procesor minimum 6 rdzeniowy osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 19500 pkt. według wyników opublikowanych na stronie <a href="http://www.cpubenchmark.net/cpu_list.php">http://www.cpubenchmark.net/cpu_list.php</a> .
Pamięć RAM	16GB DDR4, możliwość rozbudowy do min 64GB, min. 1 slot wolny
Pamięć masowa	Dysk M.2 SSD 512GB PCIe NVMe
Karta graficzna	Zintegrowana z procesorem
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, port audio combo (słuchawki + mikrofon) na panelu przednim, na tylnym audio out
Obudowa	<p>Typu SFF z obsługą kart rozszerzeń o niskim profilu, napęd optyczny w dedykowanej wnęce zewnętrznej slim. Suma wymiarów mierzona po krawędziach obudowy nie może przekraczać 70cm, waga max 6kg</p> <p>Zasilacz o mocy max. 180W pracujący w sieci 230V 50/60Hz prądu zmiennego</p> <p>Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED np. przycisku POWER ( np, migania, zmiana barw). System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię procesora.</p> <p>Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wnęk zewnętrznych 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.</p>

ZPI.271.12.2023

	<p>Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz musi być wpisany na stałe w BIOS.</p>
Zgodność z systemem operacyjnym	<p>Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (do oferty załączyć wydruk ze strony producenta oprogramowania)</p>
Bezpieczeństwo	<p>Ukryty w laminacie płyty głównej dedykowany 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.</p> <p>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</p>
BIOS	<p>BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, nazwę producenta komputera, model komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy.</p> <p>Możliwość, bez na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych oraz dodatkowego oprogramowania typu system diagnostyczny odczytania z wewnętrznego menu BIOS informacji o: wersji BIOS, nr seryjnym komputera, dacie wyprodukowania komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem obecnej, minimalnej i maksymalnej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardej, MAC adresie zintegrowanej karty sieciowej,</p> <p>Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS)</p> <p>Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznymi urządzeniami.</p> <p>Możliwość ustawienia hasła systemowego/użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) oraz uprawniającego do samodzielnej zmiany tego hasła przez użytkownika (bez możliwości zmiany innych parametrów konfiguracji BIOS) przy jednoczesnym zdefiniowanym hasle administratora.</p> <p>Możliwość wyłączenia portów USB w tym:</p>

ZPI.271.12.2023

	<p>- tylko portów USB znajdujących się na przednim panelu obudowy,</p> <p>- tylko portów USB znajdujących się na tylnym panelu obudowy.</p> <p>- wszystkich portów USB</p> <p>- pojedynczo</p>
Certyfikaty i standardy	<p>Urządzenia wyprodukowane zgodnie z normą ISO 9001 oraz ISO 50001 (certyfikaty załączyć do oferty)</p> <p>Deklaracja zgodności CE</p> <p>Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci <del>oświadczenia producenta jednostki</del> <b>dokumentacji producenta (np. certyfikat, karta katalogowa, deklaracja lub inny równoważny), dopuszcza się załączenie oświadczenia wykonawcy o spełnianiu kryterium</b> (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</p> <p>Certyfikat Energy Star 8.0 lub TCO dla oferowanego modelu – załączyć do oferty</p>
Ergonomia	<p>Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy jałowej dysku twardego (IDLE) wynosząca maksymalnie 22 dB (<del>załączyć oświadczenie producenta</del>) <b>(załączyć odpowiedni dokument potwierdzający (np. certyfikat, kartę katalogową, deklarację producenta lub inny równoważny), dopuszcza się załączenie oświadczenia wykonawcy o spełnianiu kryterium)</b></p>
System Operacyjny	<p>Zainstalowany system operacyjny Windows 11 Professional lub równoważny, klucz licencyjny musi być zapisany trwale w BIOS.</p> <p>System równoważny musi posiadać następujące cechy:</p> <p>System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:</p> <ol style="list-style-type: none"> <li>1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: <ol style="list-style-type: none"> <li>a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,</li> <li>b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych</li> </ol> </li> <li>2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego</li> <li>3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim</li> <li>4. Możliwość tworzenia pulpitu wirtualnych, przenoszenia aplikacji pomiędzy pulpitemi i przełączanie się pomiędzy pulpitemi za pomocą skrótów klawiaturowych lub GUI.</li> <li>5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe</li> <li>6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom</li> </ol>



ZPI.271.12.2023

	<p>menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,</p> <ol style="list-style-type: none"><li>7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.</li><li>8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim</li><li>9. Wbudowany system pomocy w języku polskim.</li><li>10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).</li><li>11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.</li><li>12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.</li><li>13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.</li><li>14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.</li><li>15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.</li><li>16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".</li><li>17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.</li><li>18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.</li><li>19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.</li><li>20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.</li><li>21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.</li><li>22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.</li><li>23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."</li><li>24. Wbudowany mechanizm wirtualizacji typu hypervisor."</li><li>25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.</li><li>26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.</li></ol>
--	---

ZPI.271.12.2023

	<p>27. Wbudowana zaporę internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.</p> <p>28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).</p> <p>29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niez zarządzanymi.</p> <p>30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.</p> <p>31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.</p> <p>32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM</p> <p>33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.</p> <p>34. Możliwość tworzenia wirtualnych kart inteligentnych.</p> <p>35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)</p> <p>36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.</p> <p>37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.</p> <p>38. Mechanizmy logowania w oparciu o:</p> <ol style="list-style-type: none"> <li>Login i hasło,</li> <li>Karty inteligentne i certyfikaty (smartcard),</li> <li>Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),</li> <li>Certyfikat/Klucz i PIN</li> <li>Certyfikat/Klucz i uwierzytelnienie biometryczne</li> </ol> <p>39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5</p> <p>40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.</p> <p>41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach</p> <p>42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń</p> <p>43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń</p>
Porty I/O	<p>Wbudowane porty:</p> <ul style="list-style-type: none"> <li>- panel przedni : 2x USB 3.2 gen 1, 2x USB 2.0, 1x audio (dopuszcza się combo),</li> <li>- panel tylny: 1x audio out, 2x USB 3.2 gen 1, 2x USB 2.0, 1x DP 1.4, 1x HDMI 1.4b, 1x RJ45</li> <li>- karta WiFi zamontowana w złączu miniPCIe na płycie głównej,</li> </ul>

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

### ZPI.271.12.2023

	<p>Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w : 1x PCI Express x16, 1x PCI Express x1, min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, min. 2 złącza SATA w tym 1 szt SATA 3.0, 1 złącze M.2 dla dysków SSD, 1 złącze M.2 dla bezprzewodowej karty WiFi</p>
Wymagania dodatkowe	<p>Klawiatura USB w układzie polski programisty</p> <p>Mysz optyczna USB</p> <p>Wbudowana nagrywarka DVD +/- RW</p>
Warunki gwarancji	<p>Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.</p> <p>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)</p> <p>Minimum 2-letnia gwarancja świadczona na miejscu u klienta,</p> <p>Czas reakcji serwisu - do końca następnego dnia roboczego.</p> <p>Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.</p> <p>Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.</p>
Wsparcie techniczne producenta	<p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p> <p>Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony.</p>

Monitor – 5 sztuk:

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
Monitor	Monitor będzie wykorzystywany dla potrzeb aplikacji biurowych, obróbki zdjęć lub wideo. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację monitora
Wielkość ekranu	Przekątna ekranu min. 23,5"
Matryca	Typu IPS/VA o wykończeniu matowym (nie dopuszcza się naklejek matowujących matrycę)
Czas reakcji	Maks. 8 ms

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

## ZPI.271.12.2023

Nominalna rozdzielczość i wielkość piksela	Rozdzielczość nie mniejsza niż: FHD (1920x1080)
Kąty widzenia	Kąty widzenia min. 178 stopni w pionie i w poziomie
Liczba wyświetlanych kolorów	Nie mniej niż 16,7 mln
Kontrast i jasność	Kontrast nie mniejszy niż: 3000:1 Jasność nie mniejsza niż 250 cd/m2
Porty/złącza	Minimalna ilość dostępnych złącz monitora: minimum 2 różne spośród: DisplayPort, HDMI, VGA
Kable	Wymagane kable w zestawie z monitorem min.: Kabel sygnałowy (DP/HDMI/VGA) Kabel zasilający
Podstawa monitora	Musi umożliwiać: przechylenie w pionie
Obudowa	Wbudowane w obudowę przyciski umożliwiające włączenie, wyłączenie oraz zmianę ustawień wyświetlania monitora Obudowa trwale oznaczona numerem seryjnym i katalogowym pozwalającym na jednoznaczna identyfikację zaoferowanego monitora Wbudowany zasilacz w obudowie

### Stanowisko robocze mobilne

Laptop – 15 sztuk:

Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, dostępu do Internetu oraz poczty elektronicznej,
Matryca	Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości FHD (1920 x 1080) z podświetleniem LED matryca matowa, jasność min. 220nits, kontrast 400:1
Procesor	Procesor dedykowany do pracy w komputerach mobilnych. Procesor minimum 4 rdzeniowy osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 9950 pkt. według wyników opublikowanych na stronie <a href="http://www.cpubenchmark.net/cpu_list.php">http://www.cpubenchmark.net/cpu_list.php</a>
Pamięć RAM	16 GB DDR4 możliwość rozbudowy do min 16GB, dwa sloty pamięci (nie dopuszcza się pamięci wlutowanych); możliwość rozbudowy pamięci przez użytkownika, bez kontaktu z serwisem producenta.
Pamięć masowa	min. 500 GB SSD NVMe, fabryczna możliwość instalacji drugiego dysku 2,5"
Karta graficzna	Zintegrowana z procesorem
Multimedia	Dwukanałowa karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki stereo o średniej mocy min. 2x 2W,

**ZPI.271.12.2023**

	<p>cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy.</p> <p>Kamera internetowa o rozdzielczości min. HD trwale zainstalowana w obudowie matrycy, dioda informująca użytkownika o aktywnej kamerze.</p>
Bateria i zasilanie	<p>Zasilacz o mocy min. 65W.</p> <p>Konstrukcja komputera musi umożliwiać demontaż samej baterii lub wszystkich zainstalowanych baterii, samodzielnie bez udziału serwisu w okresie gwarancyjnym. Bateria nie może być trwale zespolona z płytą główną.</p>
Waga	<p>Waga komputera z oferowaną baterią nie większa niż 1,7 kg</p>
BIOS	<p>BIOS zgodny ze specyfikacją UEFI, pełna obsługa za pomocą klawiatury i myszy.</p> <p>BIOS musi umożliwiać przeprowadzenia inwentaryzacji sprzętowej poprzez wyświetlenie informacji o: wersji BIOS, numerze seryjnym i dacie produkcji komputera, wielkości, prędkości i sposobie obsadzenia zainstalowanej pamięci RAM, typie zainstalowanego procesora, zainstalowanym dysku twardym (pojemność, model), MAC adresie wbudowanej w płytę główną karty sieciowej.</p> <p>Funkcja blokowania/odblokowania portów USB</p> <p>Możliwość, ustawienia hasła dla administratora oraz użytkownika dla BIOS'u, po podaniu hasła użytkownika możliwość jedynie odczytania informacji, brak możliwości wł/wy funkcji. Hasła silne opatrzone o litery, cyfry i znaki specjalne.</p> <p>Możliwość przypisania w BIOS numeru nadawanego przez Administratora.</p>
Bezpieczeństwo	<p>System diagnostyczny z graficzny interfejsem dostępny z poziomu BIOS lub menu BOOT'owania umożliwiający użytkownikowi przeprowadzenie wstępnej diagnostyki awarii poprzez przetestowanie: procesora, pamięci RAM, dysku, płyty głównej i wyświetlacza. Pełna funkcjonalność systemu diagnostycznego musi być dostępna również w przypadku braku lub uszkodzenia oraz sformatowania dysku twardego, braku dostępu do sieci LAN i internetu oraz nie może być realizowana przez narzędzia zewnętrzne podłączane do komputera (np. pamięć USB flash ].</p> <p>Dedykowany układ szyfrujący TPM 2.0</p> <p>Złącze na linkę zabezpieczającą przed kradzieżą.</p>
Certyfikaty	<p>Certyfikat ISO 9001 dla producenta sprzętu (załączyć do oferty)</p> <p>Certyfikat ISO 50001 dla producenta sprzętu (załączyć do oferty)</p> <p>Deklaracja zgodności CE (załączyć do oferty)</p> <p>Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci <del>oświadczenia producenta jednostki</del> <b>dokumentacji producenta (np. certyfikat, karta katalogowa, deklaracja lub inny równoważny), dopuszcza się załączenie oświadczenia wykonawcy o spełnianiu kryterium</b></p>
System operacyjny	<p>Zainstalowany system operacyjny Windows 11 Professional lub równoważny z możliwością downgrade'u do Win 10 Pro.</p>



ZPI.271.12.2023

System równoważny musi posiadać następujące cechy:  
System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
  - a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
  - b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych
2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego
3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim
4. Możliwość tworzenia pulpitu wirtualnych, przenoszenia aplikacji pomiędzy pulpitemi i przełączanie się pomiędzy pulpitemi za pomocą skrótów klawiaturowych lub GUI.
5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe
6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim
9. Wbudowany system pomocy w języku polskim.
10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.
12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.
16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.
18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.



ZPI.271.12.2023

<p>19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.</p> <p>20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.</p> <p>21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.</p> <p>22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.</p> <p>23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."</p> <p>24. Wbudowany mechanizm wirtualizacji typu hypervisor."</p> <p>25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.</p> <p>26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.</p> <p>27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.</p> <p>28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).</p> <p>29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niez zarządzanymi.</p> <p>30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.</p> <p>31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.</p> <p>32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM</p> <p>33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.</p> <p>34. Możliwość tworzenia wirtualnych kart inteligentnych.</p> <p>35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)</p> <p>36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.</p> <p>37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.</p> <p>38. Mechanizmy logowania w oparciu o:</p> <ol style="list-style-type: none"><li>Login i hasło,</li><li>Karty inteligentne i certyfikaty (smartcard),</li><li>Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),</li><li>Certyfikat/Klucz i PIN</li></ol>
--

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

**ZPI.271.12.2023**

	<p>e. Certyfikat/Klucz i uwierzytelnienie biometryczne</p> <p>39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5</p> <p>40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.</p> <p>41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach</p> <p>42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń</p> <p>43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń</p>
Wymagania dodatkowe	<p>Wbudowane porty i złącza: HDMI 1.4, RJ-45 (karta sieciowa wbudowana), min. 3xUSB w tym min. 2 port USB 3.2 gen1 typ-A, czytnik kart SD, współdzielone złącze słuchawkowe stereo i złącze mikrofonowe, złącze zasilania (zasilacz nie może zajmować portów USB)</p> <p>Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN 802.11AC, moduł bluetooth 4.1</p> <p>Klawiatura z wbudowanym podświetleniem (układ US - QWERTY) z wydzieloną klawiaturą numeryczną, touchpad z strefą przewijania w pionie, poziomie wraz z obsługą gestów.</p>
Dodatkowe oprogramowanie	<p>Dostarczone i zainstalowane w środowisku systemu operacyjnego aplikacja zapewniająca bezproblemową integrację bezprzewodową między smartfonami i komputerem. Aplikacja wspierająca zgodna z systemami iOS oraz Android 6 lub nowszy. Opatrzona w funkcjonalności:</p> <ul style="list-style-type: none"> <li>- Inicjowanie i odbieranie połączeń telefonicznych przez głośniki i mikrofon w komputerze</li> <li>- Uzyskanie dostępu do kompletnej książki telefonicznej poprzez komputer</li> <li>- Wysyłanie i odbieranie wiadomości tekstowych za pomocą klawiatury, myszy i ekranu dotykowego komputera.</li> <li>- bezprzewodowo: przeciągnij i upuść zdjęcia, filmy, muzykę i dokumenty między komputerem a smartfonem z systemem Android lub iOS.</li> <li>- tworzenie kopii lustrzanej ekranu telefonu z systemem Android lub iOS na komputerze i korzystanie z dowolnych aplikacji za pomocą klawiatury, myszy i ekranu dotykowego komputera</li> </ul>
Warunki gwarancji	<p>Minimum 2-letnia gwarancja świadczona na miejscu u klienta. Czas reakcji serwisu - do końca następnego dnia roboczego. Dedykowany portal producenta do zgłaszania awarii lub usterek, możliwość samodzielnego zamawiania zamiennych komponentów oraz sprawdzenie okresu gwarancji, fabrycznej konfiguracji.</p> <p>Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego</p> <p>Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzację producenta komputera – dokumenty potwierdzające załączyć do oferty.</p>

## ZPI.271.12.2023

	Oświadczenie oferenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych producenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
--	--

### Oprogramowanie biurowe – 11 sztuk:

Oprogramowanie biurowe z licencją wieczystą zawierające minimum:

- arkusz kalkulacyjny,
- edytor tekstu,
- program do tworzenia prezentacji,

Programy wchodzące w skład pakietu muszą w 100% odwzorowywać treść i układ dokumentów doc, docx, rtf, xls, xlsx, ppt, pptx wytworzonych w posiadanych przez Zamawiającego pakietach Microsoft Office 2016.

Edytor tekstu musi poprawnie odwzorowywać wszystkie elementy umieszczone w nagłówkach i stopkach dokumentów DOC oraz DOCX, obsługiwać osadzanie innych dokumentów tekstowych oraz arkuszy kalkulacyjnych. Dla wstawianych obiektów typu „wykres” musi istnieć możliwość osadzenia danych służących do utworzenia tego wykresu z możliwością ich edycji bezpośrednio z edytora tekstu lub poprzez otwarcie danych w dostarczonym arkuszu kalkulacyjnym. Edycja i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. Śledzenie zmian wprowadzonych przez użytkowników. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

Arkusz kalkulacyjny musi umożliwiać użycie wszystkich funkcji dostępnych w posiadanym przez Zamawiającego oprogramowaniu Microsoft Excel 2016. Arkusz kalkulacyjny musi zawierać (lub umożliwiać doinstalowanie bezpłatnego dodatku) oprogramowanie umożliwiające zoptymalizować wartość komórek zmieniających w celu uzyskania oczekiwanego rezultatu końcowego, przy jednoczesnym spełnieniu wszystkich zdefiniowanych parametrów oraz ograniczeń. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową analizę wariantową i rozwiązywanie problemów optymalizacyjnych. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. Formatowanie czasu, daty i wartości finansowych z polskim formatem. Zapis wielu arkuszy kalkulacyjnych w jednym pliku. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

Program do prezentacji musi poprawnie obsługiwać wszystkie animacje i przejścia utworzone w posiadanym przez Zamawiającego programie Microsoft Power Point 2016. Program musi umożliwiać

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

## ZPI.271.12.2023

prezentowanie przy użyciu projektora multimedialnego. Drukowanie w formacie umożliwiającym robienie notatek. Zapisanie jako prezentacja tylko do odczytu, nagrywanie narracji i dołączanie jej do prezentacji, opatrywanie slajdów notatkami dla prezentera. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, tabel i wykresów pochodzących z arkusza kalkulacyjnego. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym. Możliwość tworzenia animacji obiektów i całych slajdów. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym, monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.

### Oprogramowanie biurowe dla instytucji edukacyjnych – 9 sztuk:

Oprogramowanie biurowe z licencją wieczystą dla instytucji edukacyjnych (Szkoły oraz Biblioteka Publiczna) zawierające minimum:

- arkusz kalkulacyjny,
- edytor tekstu,
- program do tworzenia prezentacji,

Programy wchodzące w skład pakietu muszą w 100% odwzorowywać treść i układ dokumentów doc, docx, rtf, xls,xlsx, ppt, pptx wytworzonych w posiadanych przez Zamawiającego pakietach Microsoft Office 2016.

Edytor tekstu musi poprawnie odwzorowywać wszystkie elementy umieszczone w nagłówkach i stopkach dokumentów DOC oraz DOCX, obsługiwać osadzanie innych dokumentów tekstowych oraz arkuszy kalkulacyjnych. Dla wstawianych obiektów typu „wykres” musi istnieć możliwość osadzenia danych służących do utworzenia tego wykresu z możliwością ich edycji bezpośrednio z edytora tekstu lub poprzez otwarcie danych w dostarczonym arkuszu kalkulacyjnym. Edycja i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. Śledzenie zmian wprowadzonych przez użytkowników. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

Arkusz kalkulacyjny musi umożliwiać użycie wszystkich funkcji dostępnych w posiadanym przez Zamawiającego oprogramowaniu Microsoft Excel 2016. Arkusz kalkulacyjny musi zawierać (lub umożliwiać doinstalowanie bezpłatnego dodatku) oprogramowanie umożliwiające zoptymalizować wartość komórek zmienianych w celu uzyskania oczekiwanego rezultatu końcowego, przy jednoczesnym spełnieniu wszystkich zdefiniowanych parametrów oraz ograniczeń. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową analizę wariantową i rozwiązywanie problemów optymalizacyjnych. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. Formatowanie czasu, daty i wartości finansowych z polskim formatem. Zapis wielu arkuszy

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

### ZPI.271.12.2023

kalkulacyjnych w jednym pliku. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

Program do prezentacji musi poprawnie obsługiwać wszystkie animacje i przejścia utworzone w posiadanym przez Zamawiającego programie Microsoft Power Point 2016. Program musi umożliwiać prezentowanie przy użyciu projektora multimedialnego. Drukowanie w formacie umożliwiającym robienie notatek. Zapisanie jako prezentacja tylko do odczytu, nagrywanie narracji i dołączanie jej do prezentacji, opatrywanie slajdów notatkami dla prezentera. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, tabel i wykresów pochodzących z arkusza kalkulacyjnego. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym. Możliwość tworzenia animacji obiektów i całych slajdów. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym, monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.

#### Skanner A4 v1 – 1 sztuka:

Parametr	Charakterystyka (wymagania minimalne)
Rozmiar / Typ	Skanner płaski z podajnikiem ADF A4
Cechy	<ul style="list-style-type: none"> <li>• Automatyczne skanowanie dwustronne</li> <li>• Skanowanie kart zgodnych z normą ISO7810 (85.6 mm x 53.98 mm) o maksymalnej grubości 1.4 mm</li> <li>• Wykrywanie podwójnych pobrań</li> <li>• Zapis do formatów PDF, PDF/A, TIFF, wielostronicowy TIFF, Bitmapa, JPEG, JPEG2000, PNG, Word, Excel, PowerPoint</li> <li>• Funkcja monitorowania i wykrywania przekrzywionych arkuszy w celu zapobiegania ich uszkodzeniu</li> </ul>
Prędkość skanowania jednostronnego mono/kolor	min. 70 str./min
Złącza	USB 3.1 lub szybsze, LAN Gigabit
Waga skanera	maks. 8.9Kg
Głębokość szarości	min. 8bit
Pojemność ADF	min. 100 A4 80 g/m <sup>2</sup>
Rozdzielczość optyczna	600dpi lub lepsza
Obsługa gramatury papieru	min. 460 g/m <sup>2</sup>
Dzienne obciążenie	min. 10 000 stron
Pobór mocy w trybie uśpienia	maks. 2W
Źródło zasilania	100V - 240V AC
Wbudowana pamięć	min. 512MB

#### Skanner A4 v2 – 2 sztuki

Parametr	Charakterystyka (wymagania minimalne)
Typ skanera	Szczelinowy skaner dokumentów z podajnikiem ADF
Rozdz. optyczna w pionie	Minimum 600 dpi
Rozdz. optyczna w poziomie	Minimum 600 dpi

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

### ZPI.271.12.2023

Rozdz. interpolowana	Minimum 1200 x 1200 dpi
Wewnętrzna głębia koloru	Minimum 48 bit
Przyciski funkcyjne na obudowie	Tak - wymagane
Maks. szerokość skanowania	Minimum 215.9 mm
Maks. długość skanowania	Minimum 355.6 mm
Maks. szybkość skanowania	Minimum 35 str./min.
Zainstalowane opcje	automatyczny podajnik ADF (na minimum 50 arkuszy)
Interfejs	Hi-Speed USB 2.0
Waga	Maksymalnie 2,7 kg
Pobór mocy w trybie gotowości	maks. 5W
Głośność pracy	maks. 49 dB
Dodatkowe informacje	<ul style="list-style-type: none"> <li>gramatura nośników: 50 - 209 g/m<sup>2</sup></li> <li>automatyczne skanowanie dwustronne</li> <li>Możliwość skanowania bezpośrednio do OCR i e-mail</li> </ul>
Gwarancja	Min. 24 miesiące
Opcje dodatkowe	oprogramowanie do zarządzania wizytówkami i dokumentami dla systemów Windows i macOS

### Urządzenie wielofunkcyjne v1 – 1 sztuka

Nazwa komponentu/parametru	Wymagane minimalne parametry techniczne urządzenia wielofunkcyjnego
Urządzenie wielofunkcyjne kolorowe	Laserowe lub LED - Urządzenie wielofunkcyjne kolorowe A3
Procesor	1,75 GHz
Pamięć	3,5 GB
Dysk twardy	250GB SSD, opcjonalnie możliwość dołożenia dysku twardego 1TB
Interfejsy	Standardowo: 1000Base-T/100Base-TX/10Base-T, bezprzewodowa sieć LAN (IEEE 802.11 b/g/n, )USB 2.0 (host) x 1, USB 3.0 (host) x 1, USB 2.0 (urządzenie) x1
Panel sterowania	dotykowy, kolorowy, min. 10-calowy
Obsługa	Czujnik ruchu wykrywający zbliżającego się użytkownika i wybudzający urządzenie z trybu uśpienia
Prędkość drukowania	A4 mono - 26 str/min A4 kolor - 26 str/min A3 mono - 15 str/min A3 kolor - 15 str/min
Czas nagrzewania	maks. 10 sek
Rozdzielczość drukowania rzeczywista (nie interpelowana)	1200x1200 dpi
Język opisu strony	PCL 6, oryginalny Adobe PostScript3 (nie emulacja)

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

**ZPI.271.12.2023**

Dupleks	Automatyczny
Wydruk plików z pamięci USB	Obsługiwane formaty PDF, JPEG, TIFF, EPS, XPS
Wydruk ze smartfonów oraz chmury	Tak
Wydruk wstrzymany	Możliwość zdefiniowania na urządzeniu polityki wstrzymywania wszystkich lub wybranych wydruków. Możliwość zarządzania swoją kolejką wstrzymanych prac na pulpicie urządzenia, po identyfikacji użytkownika kodem PIN (opcjonalnie kartą) -podgląd wstrzymanego dokumentu, zmiana opcji wykończeniowych, zwolnienie do druku lub wykasowanie pracy.
Skaner	dwuprzebiegowy podajnik oryginałów
Rozdzielczość skanowania	600x600dpi
Pojemność podajnika dokumentów	100 arkuszy o gramaturze 80 g/m <sup>2</sup>
Prędkość skanowania w czerni i kolorze	70 obr./min przy 300dpi.
Format plików	TIFF, JPEG, PDF, PDF/A-1b, XPS
OCR	Wbudowany moduł OCR bez limitu stron i licencji pozwalający skanować do formatów Word, PowerPoint, przeszukiwalnego PDF
Skanowanie do pamięci USB oraz smartfonów	Tak
Skanowanie do chmury	Możliwość skanowania do chmury
Czas uzyskania pierwszej kopii	mono maksymalnie 6 s kolor maksymalnie 9 s
Kopiowanie ciągle	1-999
Powiększanie dokumentów	25% - 400%
Kopiowanie dwustronne	Automatyczne kopiowanie dwustronne oryginałów na dwustronne kopie.
Kasety na papier	Co najmniej 2 kasety obsługujące koperty oraz co najmniej jedna obsługująca format papieru A5R-A3
Pojemność kaset na papier	2 kasety - każda na 550 arkuszy o gramaturze 80 g/m <sup>2</sup>
Obsługiwana gramatura papieru z podajnika bocznego	52 - 300 g/m <sup>2</sup>
Podajnik boczny	na 100 arkuszy (80 g/m <sup>2</sup> ) obsługujący gramaturę 52 – 300 g/m <sup>2</sup> i formaty A5-A3, wydruk na papierze powlekanym
Pojemność tacy odbiorczej	250 arkuszy o gramaturze 80 g/m <sup>2</sup>
Finisz (Opcja)	Finisz wewnętrzny zszywający 50ark. (80g/m <sup>2</sup> ), posiadający funkcję zszywacza ekologicznego (bezszywkowego) do 4ark. oraz funkcję zszywania na żądanie min. 30 ark A4 (80g/m <sup>2</sup> )
Bezpieczeństwo	Integracja z systemem SIEM



Sfinansowano w ramach reakcji Unii na pandemię COVID-19

### ZPI.271.12.2023

Oprogramowanie	Wraz z urządzeniem dostarczone musi być oprogramowanie oparte na chmurze (bez potrzeby instalacji lokalnego serwera) do centralnego śledzenia i raportowania kosztów, generowanych przez poszczególnych użytkowników, powstałych poprzez wykonanie określonych ilości kopii/wydruków/skanów. Możliwość centralnego definiowania identyfikatorów użytkowników (numerów kart lub kodów PIN). Możliwość przydzielania uprawnień do poszczególnych funkcji urządzeń, np. kolor czy skanowanie. Możliwość rozbudowy o kolejne urządzenia tej samej marki, bez konieczności zakupu dodatkowych licencji.
Tygodniowe zużycie energii TEC zgodnie z Energy Star	nie więcej niż 1.6 kWh
Inne wymagania	Okres gwarancji wynosi 36 miesięcy. Gwarancja musi być świadczona przez autoryzowany serwis producenta urządzenia. Urządzenie musi być fabrycznie nowe i wyprodukowane nie później niż w roku 2022

### Urządzenie wielofunkcyjne v2 – 1 sztuka

Nazwa komponentu/parametru	Wymagane minimalne parametry techniczne urządzenia wielofunkcyjnego
Urządzenie wielofunkcyjne	Laserowe lub LED - Urządzenie wielofunkcyjne A4
Pamięć	1GB
Pamięć masowa	2 GB eMMC
Interfejsy	Standardowo: USB 2.0 Hi-Speed, 10BASE-T/100BASE-TX/1000Base-T/bezprzewodowa sieć LAN (IEEE 802.11 b/g/n), bezpośrednie połączenie Wi-Fi
Wyświetlacz	Kolorowy ekran dotykowy LCD TFT WVGA o przekątnej 12,7 cm / 5 cali
Prędkość drukowania - jednostronnie	A4 - min. 43str./min
Rozdzielczość drukowania	600x600 dpi
Podajnik dokumentów	jednoprzebiegowy automatyczny dwustronny podajnik dokumentów
Pojemność podajnika dokumentów	50 arkuszy ( 80g )
Prędkość skanowania	Skanowanie dwustronne (cz.-b.): 70 Skanowanie dwustronne (kol.): 26
Rozdzielczość skanowania	600x600 dpi
Skanowanie do chmury	Możliwość skanowania do chmury
Język opisu strony	PCL 6, oryginalny Adobe PostScript3
Dupleks	Automatyczny
Czas druku pierwszej strony	maksymalnie 6,4 sek.

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

### ZPI.271.12.2023

Czas nagrzewania od włączenia urządzenia	Maksymalnie 14 sek.
Kaseta na papier	Min. 1 kaseta o pojemności min.550ark. (80g/m <sup>2</sup> )
Taca wielofunkcyjna	na min. 100 arkuszy (80 g/m <sup>2</sup> ) obsługująca gramaturę 60 – 199 g/m <sup>2</sup> i formaty A6-A4 oraz obsługująca koperty: COM10, DL, C5, Monarch
Możliwość rozbudowy o dodatkowe kasety papieru	Tak - min. 3 kasety każda na 500ark. (80g/m <sup>2</sup> )
Pojemność tacy odbiorczej	150 arkuszy o gramaturze 80 g/m <sup>2</sup> - wydrukiem do dołu
Oprogramowanie	Wraz z urządzeniem dostarczone musi być oprogramowanie oparte na chmurze (bez potrzeby instalacji lokalnego serwera) do centralnego śledzenia i raportowania kosztów, generowanych przez poszczególnych użytkowników, powstałych poprzez wykonanie określonych ilości wydruków. Możliwość rozbudowy o kolejne urządzenia tej samej marki, bez konieczności zakupu dodatkowych licencji.
Inne wymagania	Urządzenie dostarczone wraz z tonerem wyprodukowanych przez producenta urządzenia: toner na min. 20.000 str (zgodnie z normą ISO/IEC 19752)
	Urządzenie musi być fabrycznie nowe i wyprodukowane w 2022 roku.

#### Słuchawki z mikrofonem – 12 sztuk

Łączność: Przewodowe

Budowa słuchawek: Nauszne

Pasma przenoszenia słuchawek: min. 42 ~ 17000 Hz

Wbudowany mikrofon: Tak, ruchomy

Złącze: Minijack 3,5 mm

Długość kabla: min. 1,8 m

Waga: max. 80g

Gwarancja producenta: min. 24 miesiące

#### Mysz bezprzewodowa – 15 sztuk

Optyczna, mysz bezprzewodowa,

Rozdzielczość min. 1000 dpi,

Trzy przyciski, rolka przewijania pionowego (trzeci przycisk może być w rolce),

Zasięg pracy min 10 m,

Zasilanie bateryjne.

Gwarancja producenta: min. 24 miesiące

#### Zasilacz UPS – 1 sztuka

Czas przełączania [ms]: max. 4

Kształt przebiegu sinus: Sinusoidalna / Sinusoida symulowana (schodkowa)

Liczba gniazd wyjściowych: min. 2

Moc pozorna [VA]: min. 850

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

## ZPI.271.12.2023

Moc skuteczna [W]: min. 480

Napięcie wejściowe (zakres) : 220 - 240

Sygnalizacja pracy: akustyczna + wyświetlacz LCD

Topologia: Line-interactive / Online

Zabezpieczenia: min. Przeciwzwarciowe, Przeciwprzepięciowe

### Router / Firewall UTM – 2 sztuki

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Wymagania Ogólne	<p>System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> <li>• Firewall.</li> <li>• Ochrony w warstwie aplikacji.</li> <li>• Protokołów routingu dynamicznego.</li> </ul>
2.	Redundancja, monitoring i wykrywanie awarii	<ol style="list-style-type: none"> <li>1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.</li> <li>2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.</li> <li>3. Monitoring stanu realizowanych połączeń VPN.</li> <li>4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.</li> </ol>
3.	Interfejsy, Dysk, Zasilanie:	<ol style="list-style-type: none"> <li>1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: <ul style="list-style-type: none"> <li>• 5 portami Gigabit Ethernet RJ-45.</li> </ul> </li> <li>2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</li> </ol>

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

**ZPI.271.12.2023**

4.	Parametry wydajnościowe	<ol style="list-style-type: none"> <li>1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.</li> <li>2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.</li> <li>3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.</li> <li>4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.</li> <li>5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.</li> <li>6. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.</li> </ol>
5.	Funkcje Systemu Bezpieczeństwa	<p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ol style="list-style-type: none"> <li>1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.</li> <li>2. Kontrola Aplikacji.</li> <li>3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.</li> <li>4. Ochrona przed malware.</li> <li>5. Ochrona przed atakami - Intrusion Prevention System.</li> <li>6. Kontrola stron WWW.</li> <li>7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.</li> <li>8. Zarządzanie pasmem (QoS, Traffic shaping).</li> <li>9. Mechanizmy ochrony przed wyciekami poufnej informacji (DLP).</li> <li>10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.</li> <li>11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.</li> <li>12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.</li> <li>13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa)</li> </ol>
6.	Polityki, Firewall	<ol style="list-style-type: none"> <li>1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</li> <li>2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: <ul style="list-style-type: none"> <li>• Translację jeden do jeden oraz jeden do wielu.</li> <li>• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.</li> </ul> </li> <li>3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</li> </ol>

ZPI.271.12.2023

		<p>4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.</p> <p>5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</p> <p>6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</p> <p>7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.</p> <ul style="list-style-type: none"> <li>• Amazon Web Services (AWS).</li> <li>• Microsoft Azure.</li> <li>• Cisco ACI.</li> <li>• Google Cloud Platform (GCP).</li> <li>• OpenStack.</li> <li>• VMware NSX.</li> <li>• Kubernetes.</li> </ul>
7.	Połączenia VPN	<p>1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> <li>• Wsparcie dla IKE v1 oraz v2.</li> <li>• Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).</li> <li>• Obsługa protokołu Diffie-Hellman grup 19, 20.</li> <li>• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.</li> <li>• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.</li> <li>• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.</li> <li>• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.</li> <li>• Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.</li> <li>• Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.</li> <li>• Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.</li> <li>• Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.</li> <li>• Mechanizm „Split tunneling” dla połączeń Client-to-Site.</li> </ul> <p>2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> <li>• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.</li> <li>• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.</li> </ul>

**ZPI.271.12.2023**

		<ul style="list-style-type: none"> <li>• Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.</li> </ul>
8.	Routing i obsługa łączą WAN	<p>W zakresie routingu rozwiązanie zapewnia obsługę:</p> <ol style="list-style-type: none"> <li>1. Routingu statycznego.</li> <li>2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).</li> <li>3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.</li> <li>4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.</li> <li>5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.</li> <li>6. BFD (Bidirectional Forwarding Detection).</li> <li>7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.</li> </ol>
9.	Funkcje SD-WAN	<ol style="list-style-type: none"> <li>1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łącz WAN.</li> <li>2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPsec).</li> </ol>
10.	Zarządzanie pasmem	<ol style="list-style-type: none"> <li>1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</li> <li>2. System daje możliwość określania pasma dla poszczególnych aplikacji.</li> <li>3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</li> <li>4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.</li> </ol>
11.	Ochrona przed malware	<ol style="list-style-type: none"> <li>1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</li> <li>2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</li> <li>3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.</li> <li>4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</li> </ol>

ZPI.271.12.2023

		<p>5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</p> <p>6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.</p> <p>8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.</p> <p>9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</p> <p>10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</p>
12.	Ochrona przed atakami	<p>1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.</p> <p>3. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>4. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p> <p>5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</p> <p>6. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.</p> <p>7. Wykrywanie i blokowanie komunikacji C&amp;C do sieci botnet.</p> <p>8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.</p>
13.	Kontrola aplikacji	<p>1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.</p> <p>3. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>4. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</p> <p>5. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).</p>

ZPI.271.12.2023

		<p>6. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).</p>
14.	Kontrola WWW	<p>1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorii tematyczne.</p> <p>2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</p> <p>3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.</p> <p>4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</p> <p>6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</p> <p>7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</p> <p>8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</p> <p>9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.</p>
15.	Uwierzytelnianie użytkowników w ramach sesji	<p>1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:</p> <ul style="list-style-type: none"> <li>• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.</li> <li>• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.</li> <li>• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.</li> </ul> <p>2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.</p> <p>3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.</p> <p>4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</p>
16.	Zarządzanie	<p>1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak</p>



ZPI.271.12.2023

		<p>i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.</p> <p>2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.</p> <p>4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</p> <p>5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p> <p>8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</p> <p>9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</p>
17.	Logowanie	<p>1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.</p> <p>2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p> <p>3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</p> <p>4. Możliwość włączenia logowania per reguła w polityce firewall.</p> <p>5. System zapewnia możliwość logowania do serwera SYSLOG.</p> <p>6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p>
18.	Serwisy i licencje	<p>Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering na okres co najmniej 12 miesięcy.</p>

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

## ZPI.271.12.2023

19.	Gwarancja oraz wsparcie	1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres co najmniej 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
-----	-------------------------	--

### Router / Firewall UTM – usługa konfiguracji wraz z rozszerzonym wsparciem technicznym – 2 sztuki

Do zamawianego sprzętu (Router / Firewall UTM) Wykonawca zapewni usługi wsparcia technicznego świadczone przez producenta lub Autoryzowanego Partnera Serwisowego Producenta świadczona w języku polskim w zakresie:

- wsparcie telefoniczne zespołu certyfikowanych inżynierów,
- pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu,
- doradztwo w zakresie konfiguracji,
- zdalne wsparcie techniczne,
- pomoc w zakładaniu zgłoszeń serwisowych u producenta,
- pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą),
- przygotowanie urządzenia do zdalnej konfiguracji,
- zdalna pierwsza konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika (dodatkowo możliwość minimum 10 zdalnych zmian konfiguracji zgodnie z wymaganiami użytkownika w okresie trwania wsparcia),

Dostęp do usługi świadczonej przez dedykowaną infolinię (należy podać numer telefonu) oraz przez dedykowany moduł internetowy (należy podać adres).

Usługa ta ma być świadczona przez podmiot posiadający certyfikat ISO 9001 w zakresie świadczenia usług serwisowych.

~~Do oferty należy załączyć oświadczenie producenta lub Autoryzowanego Dystrybutora o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001 oraz certyfikaty minimum 4 certyfikowanych inżynierów w zakresie oferowanego rozwiązania.~~

### Cyberbezpieczeństwo - szkolenie

Warsztat z bezpieczeństwa IT dla pracownika działu IT – 1 osoba.

Celem przeprowadzenia warsztatów jest przygotowanie personelu działu IT do oceny bezpieczeństwa organizacji za pomocą wybranych narzędzi.

Korzyści jakie mają wynikać z ukończenia szkolenia:

- Ocena realnego stanu bezpieczeństwa infrastruktury firmy
- Podniesienie wiedzy i umiejętności personelu technicznego odpowiedzialnego za utrzymanie systemów
- Zapoznanie się z najlepszymi praktykami związanymi z zabezpieczeniami infrastruktury IT

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

## ZPI.271.12.2023

- Poznanie wybranych narzędzi stosowanych w bezpieczeństwie IT
- Możliwość wykonywania audytów bezpieczeństwa we własnym zakresie

Język szkolenia

- Szkolenie: polski
- Materiały: polski

Minimalny zakres szkolenia:

- Wprowadzenie do warsztatów
  - Omówienie podstawowych zagadnień dotyczących bezpieczeństwa IT (terminologia, ryzyko i elementy zarządzania ryzykiem, czym jest „hardening” systemów i gdzie szukać źródeł informacji dotyczących utwardzania systemów)
- Przygotowanie do ćwiczeń
  - Omówienie środowiska laboratoryjnego (VMware Workstation, topologia sieci, systemy operacyjne)
- Elementy „białego wywiadu”
  - Omówienie gdzie i jakie informacje dotyczące firmy, jej infrastruktury oraz pracowników potencjalni intruzy mogą znaleźć w Internecie
- Skanowanie sieci i wykrywanie szczegółów dotyczących systemów operacyjnych i uruchomionych usług
  - Omówienie narzędzi wykorzystywanych przy rozpoznawaniu dostępnych systemów, usług oraz urządzeń pracujących w sieci
- Wyszukiwanie i analiza podatności
  - Omówienie przykładowych narzędzi służących do zautomatyzowanego poszukiwania podatności (np. OpenVAS) w systemach oraz wygenerowanie raportów podsumowujących poziom bezpieczeństwa testowanego środowiska
- Przelamywania zabezpieczeń systemów i urządzeń
  - Omówienie przykładowych narzędzi i sposobów przelamywania zabezpieczeń systemów. Przejmowanie podatnego systemu na przykładzie Windows, przechwytywanie haseł, obrazu z kamery, plików oraz wejścia klawiatury. Eskalacja uprawnień i przykłady ataków na Active Directory
- Bezpieczeństwo sieci bezprzewodowych i łamanie haseł
  - Analiza bezpieczeństwa sieci bezprzewodowych oraz przechwytywanie ruchu, który umożliwi łamanie haseł dostępowych. Omówienie przykładowych narzędzi. Łamanie haseł WEP i WPA2
- Socjotechniki w praktyce

Omówienie wybranych narzędzi wykorzystywanych w atakach socjotechnicznych, przygotowanie środowiska do kampanii socjotechnicznej