

Znak postępowania: Or.271.6.2022

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Część 4 pn.: Dostawa stacji roboczych AiO oraz dostawa oprogramowania antywirusowego

Przedmiotem zamówienia jest dostawa **5 szt. stacji roboczych AiO** oraz dostawa **35 szt. licencji oprogramowania antywirusowego**

1. Wymagane minimalne parametry techniczne/jakościowe komputerów:

L.p.	Parametr lub warunek	Wymagane minimalne parametry techniczne/jakościowe komputerów
1.	Typ	Komputer stacjonarny typu All in One, komputer fabrycznie wbudowany w obudowę monitora. W ofercie wymagane jest podanie modelu producenta komputera.
2.	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji bazodanowych, dostępu do Internetu oraz poczty elektronicznej,
3.	Wydajność obliczeniowa	Procesor wielordzeniowy osiągający w teście PassMark CPU Mark wynik min. 12000 punktów według wyników ze strony https://www.cpubenchmark.net na dzień składania ofert.
4.	Pamięć RAM	8GB DDR4 możliwością rozbudowy do 32GB, jeden slot wolny.
5.	Pamięć masowa	500GB SSD
6.	Wydajność grafiki	Grafika zintegrowana z procesorem
7.	Matryca	<ol style="list-style-type: none"> 1. Rozmiar matrycy min.21.5", IPS lub WVA lub MVA. 2. Rozdzielczość FHD (1920x1080). 3. Jasność typowa min. 250 cd/m². 4. Kontrast typowy 1000:1. 5. Kąty widzenia 170 / 170 stopni.
8.	Wyposażenie multimedialne	<ol style="list-style-type: none"> 1. Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki min. 3W na kanał. 2. Wbudowany w obudowę mikrofon. 3. Wbudowana kamera HD ze zintegrowaną przesłoną mechaniczną umożliwiającą jej fizyczne zasłonięcie.
9.	Obudowa	<ol style="list-style-type: none"> 1. Typu All-in-One zintegrowana z monitorem min. 21,5". 2. Podstawa musi umożliwiać regulację kąta w pionie w zakresie -5 do 30 stopni
10.	System diagnostyczny	Wbudowany system diagnostyczny działający niezależnie od uszkodzenia dysku twardego z systemem operacyjnym komputera, umożliwiający na wykonanie diagnostyki następujących podzespołów: <ul style="list-style-type: none"> - wykonanie testu pamięci RAM - test dysku twardego wraz z możliwością wyświetlania danych SMART

		<ul style="list-style-type: none"> - test matrycy LCD - test magistrali PCI-e - test portów USB - test CPU - test myszy i klawiatury
11.	Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą poprawnie współpracować z oferowanymi systemami operacyjnymi (dokument potwierdzający certyfikację należy dostarczyć w trakcie dostawy).
12.	BIOS	<p>1. BIOS zgodny ze specyfikacją UEFI,</p> <p>2. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:</p> <ul style="list-style-type: none"> - modelu komputera, producencie komputera, - numerze seryjnym, - numerze inwentarzowym, - MAC Adres karty sieciowej, - wersja Biosu wraz z datą produkcji, - ilości pamięci RAM - napędach lub dyskach podłączonych do portów SATA oraz M.2 (model dysku twardego i napędu optycznego), <p>3. Możliwość z poziomu Bios:</p> <ul style="list-style-type: none"> - wyłączenia portów USB, - wyłączenia wbudowanej kamery, karty WiFi, karty audio, mikrofonu, głośników, czytnika kart, - włączania/wyłączania trybu PXE, - włączania/wyłączania obsługi TPM, - ustawienia hasła: administratora, Power-On
13.	Certyfikaty i standardy	<ol style="list-style-type: none"> 1. Urządzenia muszą być wyprodukowane zgodnie z normą ISO 9001 2. Deklaracja zgodności CE 3. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki. <p>Wymagane certyfikaty i deklaracje należy dostarczyć w trakcie dostawy</p>
14.	System operacyjny	<p>Zainstalowany system operacyjny Windows 10/11 Pro lub równoważny.</p> <p>Zasady równoważności systemu:</p> <ol style="list-style-type: none"> 1. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek. 2. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu.

		<p>3. Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat)</p> <p>4. Internetowa aktualizacja zapewniona w języku polskim.</p> <p>5. Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.</p> <p>6. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi).</p> <p>7. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.</p> <p>8. Interfejs użytkownika działający w trybie graficznym, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta.</p> <p>9. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu.</p> <p>10. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową Active Directory.</p> <p>11. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.</p> <p>12. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.</p> <p>13. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych.</p> <p>14. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.</p> <p>15. Wbudowany system pomocy w języku polskim.</p> <p>16. Certyfikat producenta oprogramowania na dostarczany sprzęt.</p> <p>17. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).</p> <p>18. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.</p> <p>19. Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.</p>
--	--	---

		<p>20. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.</p> <p>21. System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.</p> <p>22. Wsparcie dla Sun Java i .NET Framework – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.</p> <p>23. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.</p> <p>24. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika w celu rozwiązania problemu z komputerem.</p> <p>25. Możliwość zbudowania obrazu systemu wraz z aplikacjami. Rozwiązanie to ma umożliwiać szybką instalację systemu poprzez sieć komputerową.</p> <p>26. Graficzne środowisko instalacji i konfiguracji.</p> <p>27. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.</p> <p>28. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.</p> <p>29. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.</p> <p>30. Możliwość przywracania plików systemowych.</p> <p>31. System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).</p> <p>32. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).</p> <ul style="list-style-type: none"> • Możliwość bez zastosowania dodatkowych aplikacji oraz środowisk programistycznych instalacji oraz użytkowanie aplikacji posiadanych przez Zamawiającego takich jak: Płatnik, Bestia, oprogramowanie firmy INFO-SYSTEM. • Klucz licencyjny oprogramowania systemowego musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego • Zainstalowany system operacyjny nie wymaga aktywacji za pomocą telefonu lub Internetu
--	--	---

15.	Oprogramowanie pakietu aplikacji biurowych.	<p>Fabrycznie zainstalowany MS Office 2021 dla Użytkowników Domowych i Małych Firm z dostarczoną kluczem aktywacyjnym na licencji wieczystą lub równoważny.</p> <p>Zasady równoważności:</p> <ol style="list-style-type: none"> Oprogramowanie musi umożliwiać bezpośrednie tworzenie aktów prawnych na potrzeby aplikacji Legislator (używanej przez Zamawiającego). Oprogramowanie powinno być w wersji oficjalnej, niedopuszczalne jest dostarczenie w wersji typu alpha, beta, Community Preview (CP) lub innej, która zabrania używania oprogramowania przez urząd administracji publicznej. Wymagania odnośnie interfejsu użytkownika: <ol style="list-style-type: none"> Pełna polska wersja językowa interfejsu użytkownika oraz dokumentacja i pomoc w języku polskim, Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową Active Directory – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: <ol style="list-style-type: none"> posiada kompletny i publicznie dostępny opis formatu ma zdefiniowany układ informacji w postaci XML umożliwia wykorzystanie schematów XML Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleczeń, język skryptowy). Pakiet zintegrowanych aplikacji biurowych musi zawierać min.: <ol style="list-style-type: none"> edytor tekstów arkusz kalkulacyjny narzędzie do przygotowywania i prowadzenia prezentacji aplikację do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) Edytor tekstów musi umożliwiać <ol style="list-style-type: none"> Edycję 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, Wstawianie oraz formatowanie tabel, Wstawianie oraz formatowanie obiektów graficznych, Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne), Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,
-----	---	---

		<p>8.6. Automatyczne tworzenie spisów treści</p> <p>8.7. Formatowanie nagłówków i stopek stron</p> <p>8.8. Sprawdzanie pisowni w języku polskim</p> <p>8.9. Śledzenie zmian wprowadzonych przez użytkowników</p> <p>8.10. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności</p> <p>8.11. Określenie układu strony (pionowa/pozioma),</p> <p>8.12. Wydruk dokumentów</p> <p>8.13. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną,</p> <p>8.14. Pracę na dokumentach utworzonych przy pomocy Microsoft Word w wersjach 2013÷2021 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu</p> <p>8.15. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji</p> <p>8.16. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem</p> <p>8.17. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa,</p> <p>9. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych;</p> <p>10. Arkusz kalkulacyjny musi umożliwiać:</p> <p>10.1. Tworzenie raportów tabelarycznych</p> <p>10.2. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych</p> <p>10.3. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu</p> <p>10.4. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice),</p> <p>10.5. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych</p> <p>10.6. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych</p> <p>10.7. Wyszukiwanie i zamianę danych</p>
--	--	--

		<p>10.8. Wykonywanie analiz danych przy użyciu formatowania warunkowego</p> <p>10.9. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie</p> <p>10.10. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności</p> <p>10.11. Formatowanie czasu, daty i wartości finansowych z polskim formatem,</p> <p>10.12. Zapis wielu arkuszy kalkulacyjnych w jednym pliku</p> <p>10.13. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel w wersjach 2013÷2021, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleczeń</p> <p>11. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji;</p> <p>12. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:</p> <p>12.1. Przygotowywanie prezentacji multimedialnych</p> <p>13.2. Prezentowanie przy użyciu projektora multimedialnego</p> <p>13.3. Drukowanie w formacie umożliwiającym robienie notatek</p> <p>13.4. Zapisanie jako prezentacja tylko do odczytu</p> <p>13.5. Nagrywanie narracji i dołączanie jej do prezentacji</p> <p>13.6. Opatrywanie slajdów notatkami dla prezentera</p> <p>13.7. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo</p> <p>13.8. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym</p> <p>13.9. Możliwość tworzenia animacji obiektów i całych slajdów</p> <p>13.10. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera</p> <p>13.11. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania Microsoft PowerPoint w wersjach 2013÷2021.</p> <p>13. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:</p> <p>13.1. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego</p> <p>13.2. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców</p> <p>13.3. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną</p> <p>13.4. Automatyczne grupowanie poczty o tym samym tytule</p> <p>13.5. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy</p> <p>13.6. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia</p> <p>13.7. Zarządzanie kalendarzem</p> <p>13.8. Udostępnianie kalendarza innym użytkownikom</p> <p>13.9. Przeglądanie kalendarza innych użytkowników</p>
--	--	---

		<p>13.10. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach</p> <p>13.11. Zarządzanie listą zadań</p> <p>13.12. Zlecanie zadań innym użytkownikom</p> <p>13.13. Zarządzanie listą kontaktów</p> <p>13.14. Udostępnianie listy kontaktów innym użytkownikom</p> <p>13.15. Przeglądanie listy kontaktów innych użytkowników</p> <p>13.16. Możliwość przysyłania kontaktów innym użytkownikom</p> <p>Zamawiający nie dopuszcza zaoferowania subskrypcji licencyjnej opartej o rozwiązanie chmurowe</p> <p>W przypadku błędnego działania środowiska lub wykrytych niezgodności pod kątem spełnienia warunków OPZ po instalacji oprogramowania równoważnego, Zamawiający ma prawo odstąpić od umowy.</p>
16.	Wymagania dodatkowe	<p>Wbudowane porty i złącza:</p> <ol style="list-style-type: none"> 1. min. 5 x USB. Wymagana ilość i rozmieszczenie portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, adapterów itp. 2. port sieciowy RJ-45, 3. Wbudowany moduł TPM 2.0 4. porty audio: wyjście słuchawek + wejście mikrofonowe tzw. port COMBO audio. 5. Karta sieciowa 10/100/1000 Ethernet RJ 45 (zintegrowana). 6. Klawiatura USB w układzie polski programisty 7. Mysz optyczna USB z min. dwoma klawiszami oraz rolką (scroll).
17.	Warunki gwarancji Wsparcie techniczne	<ul style="list-style-type: none"> • 2 lata Gwarancja minimalna • 3 lata Gwarancja maksymalna <p>Okres gwarancji jest ocenianym kryterium wyboru oferty.</p> <p>Gwarancja producenta świadczona na miejscu u klienta, czas reakcji serwisu - do końca następnego dnia roboczego.</p> <p>Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera.</p> <p>Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta</p>

Wymagania ogólne dotyczące sprzętu:

- 1) Wszystkie dostarczone urządzenia muszą być fabrycznie nowe, bez wad i uszkodzeń, nieregenerowane, nieużywane i nie będące przedmiotem wystaw i prezentacji oraz o ile nie wyspecyfikowano inaczej w wymaganiach szczegółowych dla urządzeń, wyprodukowane nie wcześniej niż 2021 roku.
- 2) Wszystkie urządzenia będą pochodziły z oficjalnego, europejskiego kanału dystrybucji.
- 3) Urządzenia zostaną dostarczone przez Wykonawcę własnym transportem i na własny koszt do siedziby Zamawiającego, od poniedziałku do piątku w godzinach 7:15 – 14:00 (termin dostawy należy uzgodnić z Zamawiającym).

- 4) Wszystkie urządzenia muszą być dostarczone w oryginalnych opakowaniach producenta,
- 5) Wszystkie urządzenia powinny być zgodne z normami UE i przeznaczone na rynek UE, oraz powinny posiadać certyfikat CE.
- 6) Dostarczany sprzęt powinien być kompletny i gotowy do uruchomienia, tak aby nie był konieczny zakup dodatkowych elementów czy akcesoriów,
- 7) Wykonawca dostarczy stosowne potwierdzenie gwarancji sprzętu i oprogramowania zapewniające, że sprzęt objęty jest gwarancją producenta
- 8) Serwis sprzętu będzie świadczony przez producenta lub jego autoryzowanego partnera serwisowego posiadającego wdrożoną normę min. PN-EN ISO 9001 lub równoważną.
- 9) Sprzęt dostarczany w ramach niniejszego zamówienia, powinien być objęty gwarancją i wsparciem producenta. W okresie gwarancji Wykonawca jest zobowiązany zapewnić Zamawiającemu:
 - a. usuwanie wszelkich wad i nieprawidłowości powstałych na wskutek standardowej i zgodnej z przeznaczeniem eksploatacji przedmiotu zamówienia
 - b. przyjmowanie zgłoszeń serwisowych w godzinach 8.00-20.00 (faks lub e-mail) z możliwością zgłaszania awarii bezpośrednio u producenta (na wypadek braku reakcji serwisowej ze strony Wykonawcy)
 - c. dostęp do bezpośredniego wsparcia technicznego producenta wraz z prawem do aktualizacji oprogramowania systemowego
- 10) W ramach gwarancji wymagane jest wsparcie producenta sprzętu, a czas reakcji na zgłoszenia będzie realizowany w trybie następnego dnia roboczego w miejscu instalacji i zastrzeżeniem, że uszkodzone nośniki danych pozostają u Zamawiającego. Ponadto wymagane jest, aby dostarczony poziom wsparcia producenta dawał możliwość kategoryzacji zgłoszeń i w przypadku awarii krytycznych gwarantował natychmiastową pomoc telefoniczną, szybką interwencję specjalisty ds. eskalacji zgłoszeń oraz wizytę serwisanta i/lub wysyłkę uszkodzonych części
- 11) Udzielona gwarancja producenta nie wyłącza uprawnień Zamawiającego z tytułu rękojmi w stosunku do Wykonawcy.
- 12) Zamawiający wymaga aby wszystkie dostarczone komputery były takie same, tj. pochodziły od tego samego producenta i miały ten sam typ/model. Zamawiający nie dopuszcza dostawy sprzętu powystawowego, poleasingowego, typu refurbished itp.
- 13) Wszystkie wymagania określone w niniejszym OPZ stanowią wymagania minimalne, a ich spełnienie jest obligatoryjne. Niespełnienie wyżej wymienionych wymagań minimalnych będzie skutkować odrzuceniem oferty jako niezgodnej z warunkami zamówienia na podstawie art. 226 ust. 1 pkt. 5 ustawy Pzp.

2. Oprogramowanie Antywirusowe – 35 szt. licencji stanowiskowych na okres minimum 12 miesięcy

Parametr	Charakterystyka (wymagania minimalne)
Administracja zdalna	<ol style="list-style-type: none"> 1. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. 2. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. 3. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.

	<ol style="list-style-type: none"> 4. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. 5. Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android. 6. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci. 7. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe). 8. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. 9. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 10. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora. 13. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. 14. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
Ochrona stacji roboczych	<ol style="list-style-type: none"> 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11). 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.

9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.

10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.

15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: 11

- tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
- tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
- tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
- tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
- tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

17. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

	<p>18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.</p> <p>19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).</p> <p>20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>21. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.</p> <p>22. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:</p> <ul style="list-style-type: none"> • tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, • tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, • tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, • tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. <p>23. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.</p> <p>24. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika</p> <p>25. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.</p> <p>26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.</p> <p>27. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii</p>
Ochrona serwera	<p>1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych</p> <p>2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.</p> <p>3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.</p> <p>4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.</p> <p>5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.</p>

6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).

11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.

12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

14. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.

15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.

16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.

19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.

20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Ochrona urządzeń
mobilnych opartych o
system android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
 - a. usunięcie zawartości urządzenia,
 - b. przywrócenie urządzenia do ustawień fabrycznych,
 - c. zablokowania urządzenia,
 - d. uruchomienie sygnału dźwiękowego,
 - e. lokalizację GPS.
6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
 - a. nazwę aplikacji,
 - b. nazwę pakietu,
 - c. kategorię sklepu Google Play,
 - d. uprawnienia aplikacji,
 - e. pochodzenie aplikacji z nieznanego źródła.