DZP/381/45B/2019 Załącznik nr 5 do SIWZ (załącznik nr 3 do umowy)

ZESTAWIENIE PARAMETRÓW TECHNICZNYCH

**Pakiet 1: Zestawy komputerowe - typu All-in-One**

64 sztuki, w tym:

dla lokalizacji Ceglana – 32 sztuki

dla lokalizacji Ligota – 32 sztuki

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagania minimalne – parametry techniczne komputerów** | **Faktycznie (oferowane) przez Wykonawcę parametry** |
|  | **Zestaw komputerowy - typu All-in-One** **Producent, Typ/Model: zgodnie z wypełnionym formularzem asortymentowo cenowym.** |
| 1 | **Zastosowanie:** |
|  | Komputer wykorzystywany dla potrzeb aplikacji biurowych, a w szczególności systemu InfoMedica/AMMS produkcji Asseco Poland (posiadanym przez Zamawiającego). | TAK / NIE\* |
| 2 | **Procesor:** |  |
|  | Procesor wielordzeniowy przeznaczony do komputerów stacjonarnych stosowanych w rozwiązaniach biznesowych. Musi umożliwiać obsługę zarówno 32-bitowych jak i 64-bitowych aplikacji oraz posiadać sprzętowe wsparcie wirtualizacji. Oferowany procesor ma osiągnąć wydajność min 11900 pkt. w benchmarku PassMark High End CPU’s: znajdującego się na stronie https://www.cpubenchmark.net/high\_end\_cpus.html) - wg załączonego wydruku z dnia 28.05.2019 z stanowiącego załącznik nr 9 do SIWZ)***W przypadku zaoferowania procesora, który nie będzie widniał w załączniku nr 9 do SIWZ lub w przypadku użycia przez oferenta innych testów wydajności niż wskazane przez Zamawiającego Wykonawca na wezwanie Zamawiającego na podstawie art. 26 ust 2 lub 3 ustawy PZP będzie zobowiązany złożyć oprogramowanie testujące, testowany zestaw (tj. oferowany przez Wykonawcę sprzęt w ilości 1 szt. do zwrotu Wykonawcy) oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia****. .*Procesor musi wspierać technologie udostępniania informacji o podzespołach komputera i jego oprogramowaniu, zdalnego dostępu do komputera (monitoring, sterowanie nim, konserwację niezależnie od stanu systemu operacyjnego nawet w gdy komputer jest wyłączony), oraz sprzętowe wsparcie pamięci transakcyjnej. | TAK / NIE\*Podać producenta i typ/model procesora…………………………… |
| 3 | **Płyta główna** |  |
|  | Dedykowana do komputera typu All-In-One (przeznaczona do rozwiązań biznesowych i profesjonalnych). Dostosowana do oferowanego procesora, umożliwiająca obsługę magistrali zainstalowanego procesora, wysokowydajnej pamięci zgodnej z oferowanym procesorem. | TAK / NIE\*Podać producenta i typ/model płyty …………………………… |
| 4 | **Pamięć RAM** |  |
|  | Min. 16 GB pamięci RAM w technologii zgodnej z zainstalowanym procesorem z możliwością rozszerzenia do 32GB (co najmniej 1 wolne złącze pamięci RAM) | TAK / NIE\*Podać producenta i typ/model pamięci …………………………… |
| 5 | **Dysk twardy** |  |
|  | Min. 250GB GB w technologii SSD, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego po awarii bez dodatkowych nośników.  | TAK / NIE\*Podać producenta i typ/model dysku …………………………… |
| 6 | **Karta graficzna** |  |
|  | Z akceleracją 2D/3D. Wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki, możliwość osiągnięcia rozdzielczości 1920x1080 pikseli z maksymalną głębia kolorów 32 bpp. | TAK / NIE\*Podać producenta i typ/model karty …………………………… |
| 7 | **Karta dźwiękowa / multimedia** |  |
|  | - Karta dźwiękowa zintegrowana z płytą główną, zgodna z HDA- Wbudowane głośniki stereo | TAK / NIE\* |
| 8 | **Komunikacja** |  |
|  | - Zintegrowany z płytą główną kontroler LAN Ethernet obsługujący standardy 10/100/1000 Mbits z obsługą VLAN 802.1q- Kontroler WIFI 802.11b/g/n lub 802.11ac z anteną wbudowaną w obudowę komputera- Kontroler bluetooth**Żaden z powyższych kontrolerów nie może być podłączony do komputera poprzez złącze USB.** | TAK / NIE\* |
| 9 | **Porty** |  |
|  | Zaoferowany komputer musi posiadać minimum:* 1 x DP lub HDMI
* 1 x RJ-45
* 5 portów USB (w tym co najmniej 3 porty USB 3.0)
* 1 x Audio
* 1 x port szeregowy RS232

Wymagana ilość (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, hubów itp.  | TAK / NIE\* |
| 10 | **Peryferia** |  |
|  | - Klawiatura przewodowa (długość kabla min 1.4 m) USB w układzie polski programisty - Mysz optyczna przewodowa (długość kabla min 1.4 m) USB z rolką, DPI minimum 1000 | TAK / NIE\* |
| 11 | **Napęd optyczny** |  |
|  | Wbudowana nagrywarka DVD +/-RW | TAK / NIE\* |
| 12 | **Ekran** |  |
|  | Ekran musi posiadać minimalne parametry:- rozdzielczość FULL HD 1920x1080- przekątna 21,5 cala- matryca matowa typu: IPS/VA/MVA/WVA- 16 mln kolorów- kontrast statyczny 1000:1 | TAK / NIE\*Podać producenta i typ/model matrycy …………………………… |
| 13 | **Obudowa** |  |
|  | Wielofunkcyjna typu All-In-One, musi posiadać:- możliwość montażu na ścianie z wykorzystaniem otworów montażowych w standardzie VESA- możliwość bez narzędziowego demontażu stopy- zasilacz posiadający certyfikat 80 PLUS potwierdzony spełnieniem tego wymogu zamieszczonym na stronie pod adresem: https://plugloadsolutions.com/80pluspowersupplies.aspx- czujnik otwarcia obudowy- wbudowane przyciski regulacji jasności obrazuPodstawa musi umożliwiać:- regulację kąta nachylenia w zakresie od 5st do przodu do 45st do tyłu- regulacje wysokości w zakresie minimum 100mm- regulację w poziomie w zakresie od 45st w lewo do 45st w prawo | TAK / NIE\* |
| 14 | **Zabezpieczenia fizyczne** |  |
|  | Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego np. w postaci blokady zabezpieczającej typu Kensington lub innej | TAK / NIE\* |
| 15 | **Zasilanie i eksploatacja** |  |
|  | Urządzenie spełnia wymagania rozporządzenia Komisji (UE) Nr 617/2013 w sprawie wykonania dyrektywy Parlamentu Europejskiego i Rady 2009/125/WE, posiada oznakowanie CE i wydaną deklarację zgodności WE (załącznik VI do dyrektywy 2009/125/WE) | TAK / NIE\* |
| 16 | **System operacyjny** |  |
|  | Zainstalowany system operacyjny wg wymagań wyszczególnionych poniżej z licencją dożywotnią**Wymagania dla systemu:****DOTYCZY WSZYSTKICH KOMPUTERÓW ( tj. 64 licencji )**Preinstalowany fabrycznie na dysku twardym system operacyjny w polskiej wersji językowej. System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:1. Możliwość pracy w systemie Infomedica/AMMS produkcji Asseco Poland (posiadanym przez Zamawiającego)
2. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek
3. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu
4. Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW
5. Internetowa aktualizacja zapewniona w języku polskim
6. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6
7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe
8. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi)
9. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer
10. Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta
11. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu
12. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników
13. 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
14. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych
15. Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego
16. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika
17. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi
18. Wbudowany system pomocy w języku polskim
19. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących)
20. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji
21. Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny
22. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509
23. Wsparcie dla logowania przy pomocy smartcard
24. Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji
25. System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk
26. Wsparcie dla Java i .NET Framework 1.1 i 2.0 i 3.0 i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach
27. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń
28. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem
29. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację
30. Graficzne środowisko instalacji i konfiguracji
31. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe
32. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
33. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej
34. Możliwość przywracania plików systemowych
35. 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.)

Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu | TAK / NIE\*Podać producenta i nazwę zaoferowanego oprogramowania ……………………………dot. podpunktu 3podać nazwę strony serwera WWW ………………………… |
| 17 | **Pakiet antywirusowy DOTYCZY WSZYSTKICH KOMPUTERÓW DLA LOKALIZACJI CEGLANA ( tj. 32 licencje ). Nie dotyczy lokalizacji Ligota**  |  |
|  | ***Informacja Zamawiającego:**** Zamawiający obecnie posiada pakiet antywirusowy ESET Endpoint Security do użytku dla biznesu (**381** licencji w lokalizacji Ceglana ważnych do 5.09.2020r) wraz z wdrożoną konsolą do centralnego zarządzania,
* Użyte przez Zamawiającego wszelkie nazwy handlowe, znaki towarowe, patenty i miejsce pochodzenia są uzasadnione specyfiką przedmiotu zamówienia i mają na celu wskazanie jedynie jakości przedmiotu zamówienia.

***Wymagania ogólne:**** Udzielona licencja powinna umożliwić użytkowanie programu we wszystkich jednostkach organizacyjnych Zamawiającego.
* W przypadku zaoferowania ESET Endpoint Security Suite, zamawiający wymaga, by licencja była dostarczona w formie rozszerzenia klucza dla **381** licencji przytoczonych powyżej, o ilość równą ilości zamawianych komputerów dla lokalizacji Ceglana **tj. 32 licencje z okresem ważności jak posiadany klucz przez Zamawiającego - Identyfikator publiczny 333-99N-HA7**,
* W przypadku zaoferowania innego pakietu antywirusowego niż obecnie posiadany przez Zamawiającego wymaga się, aby współpracował on z konsolą centralnego zarządzania posiadaną i wdrożoną przez Zamawiającego ESET Remote Administrator Console. Poniżej Zamawiający wskazuje wymagania minimalne dla pakietu antywirusowego:

***Wymagania ogólne dla stacji roboczych:*** * Pełne wsparcie dla zaoferowanego systemu operacyjnego
* Wersja programu dostępna w całości w języku polskim
* Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim

***Ochrona antywirusowa i antyspyware:**** Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
* Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
* Wbudowana technologia do ochrony przed rootkitami.
* Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
* Możliwość skanowania całego dysku, dysków sieciowych oraz nośników zewnętrznych wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
* System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak - nie wykonywało danego zadania.
* Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami, (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
* Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
* Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
* Skanowanie plików spakowanych i skompresowanych.
* Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).
* Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
* Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
* Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
* W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
* Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
* Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
* 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).
* Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym.
* Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.
* Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
* Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
* Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.
* Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
* Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
* Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
* Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
* Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
* Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
* Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
* Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
* Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
* W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.
* Wbudowane dwa niezależne moduły heurystyczne - jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej i/lub obu metod jednocześnie.
* Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
* Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
* Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
* Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
* Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
* Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik komputera przy próbie dostępu do konfiguracji był proszony o podanie hasła.
* Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
* Możliwość zabezpieczenia hasłem konfiguracji programu oraz jego nieautoryzowanej próby deinstalacji
* Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji - poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
* Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
* Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
* System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
* Program ma umożliwiać 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
* Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
* Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.
* Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
* W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
* Użytkownik ma posiadać możliwość takiej konfiguracji aplikacji aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
* Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
* Moduł HIPS musi posiadać możliwość pracy w jednym z czterech trybów:
* tryb automatyczny z regułami gdzie aplikacja automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
* tryb interaktywny, w którym to aplikacja 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 aplikacja uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu aplikacja musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
* Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
* Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
* Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
* Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
* Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
* Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
* Aplikacja musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
* Aplikacja musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http
* Aplikacja musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
* Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
* Program ma wspierać technologię CISCO NetWork Access Control.
* Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
* W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór następujących modułów do instalacji: ochrona antywirusowa i antyspywerowa, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, kopia dystrybucyjna

***Ochrona przed spamem:*** * Ochrona antyspamowa dla różnych programów pocztowych wykorzystująca filtry Bayes-a, białą i czarną listę oraz bazę charakterystyk wiadomości spamowych.
* Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
* Integracja z różnymi programami pocztowymi - antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego.
* Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
* Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym.
* Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam.
* Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam.
* Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana” oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana”.
* Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

***Zapora osobista (personal firewall):*** * Zapora osobista ma pracować jednym z 5 trybów:
* tryb automatyczny - program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące,
* tryb automatyczny z wyjątkami - działa podobnie jak tryb automatyczny, ale umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł,
* tryb interaktywny - program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo),
* tryb oparty na regułach - użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany,
* tryb uczenia się - umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji.
* Możliwość tworzenia list sieci zaufanych.
* Możliwość dezaktywacji funkcji zapory sieciowej na kilka sposobów: pełna dezaktywacja wszystkich funkcji analizy ruchu sieciowego, tylko skanowanie chronionych protokołów oraz dezaktywacja do czasu ponownego uruchomienia komputera.
* Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
* Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję.
* Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń.
* Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.
* Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.
* Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
* Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.
* Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
* Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
* Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci
* Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
* Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, aktywności wyłącznie jednego połączenia sieciowego lub wielu połączeń sieciowych konkretny interfejs sieciowy w systemie.
* Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6
* Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci.
* Możliwość aktualizacji sterowników zapory osobistej po restarcie komputera.

***Kontrola dostępu do stron internetowych:**** Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.
* Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
* Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
* Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
* Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i pod kategorii.
* Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
* Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta.
* Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.
 | TAK / NIE\*Podać producenta i nazwę zaoferowanego oprogramowania …………………………… |
| 18 | **Pakiet biurowy** | Nie dotyczy |
| 19 | **Gwarancja** |  |
|  | **Komputer musi posiadać pakiet serwisowy oferujący następujące warunki gwarancji:*** Gwarancja min. 36 miesięcy na części i czynności serwisowe (gwarancja na miejscu u klienta z czasem reakcji do końca następnego dnia roboczego od zgłoszenia.)
* Czas usunięcia awarii w okresie gwarancji max 14 dni roboczych (zgodnie z zadeklarowanym terminem w formularzu ofertowym) od momentu pisemnego zgłoszenia awarii, sprzęt do naprawy i z naprawy Wykonawca dostarcza na swój koszt, W przypadku awarii dysku twardego lub komputera dysk pozostaje u Zamawiającego
* Komputer nie będzie posiadał plomb lub innych elementów ograniczających dostęp do wnętrza
* Firma serwisująca musi być autoryzowanym serwisem producenta komputera
* Wykonawca zobowiązany jest do wskazania danych kontaktowych do zgłaszania awarii sprzętu
* Możliwość pobierania dokumentacji i sterowników z jednej lokalizacji w sieci Internet
* Możliwość uzyskania pomocy technicznej producenta w języku polskim za pomocą strony WWW, telefonicznie np. infolinii itp.
* Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera
* Możliwość weryfikacji czasu obowiązywania gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera
* Oświadczenie producenta komputera, że w przypadku nie wywiązania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem
 | TAK / NIE\*Uzupełnić:……….. miesięcy na miejscu u klienta z czasem reakcji do końca następnego dnia roboczego od zgłoszeniaUzupełnić:Dane kontaktowe do zgłaszania awarii:………………………..………………………..………………………..Dane kontaktowe do weryfikacji czasu obowiązywania gwarancji:………………………..………………………..……………………….. |
| 19 | **Inne, ergonomia** |  |
|  | - Produkt musi być fabrycznie nowy. Niedozwolone jest oferowanie sprzętu z programów Refurbished itp.- Certyfikat producenta oprogramowania systemu operacyjnego na konkretnie oferowany sprzęt **(***Wykonawca będzie zobowiązany złożyć na wezwanie Zamawiającego na podstawie art. 26 ust 2 lub 3 ustawy PZP)*- Certyfikat ISO 9001:2000 dla producenta sprzętu (*Wykonawca będzie zobowiązany złożyć na wezwanie Zamawiającego na podstawie art. 26 ust 2 lub 3 ustawy PZP)*- Kabel zasilający | TAK / NIE\* |
|  | **Wyposażenie dodatkowe (peryferia)**Konwerter z USB na RS232 wraz z niezbędnymi sterownikami, jeśli takowe są wymagane do prawidłowego funkcjonowania w zaoferowanym systemie operacyjnym min. 10 sztuk  | TAK / NIE\****Podać producenta i nazwę zaoferowanego konwertera: …………………………*** |

**\* niewłaściwe skreślić lub właściwe zaznaczyć**

1. W kolumnie „Faktyczne (oferowane przez Wykonawcę) parametry” w pozycjach TAK/NIE\* zaznaczanie odpowiedzi NIE oznacza niespełnienie wymaganych przez Zamawiającego parametrów.
2. Zamawiający zastrzega sobie możliwość rozbudowy komputera, bez powiadomienia o tym Wykonawcy bez utraty gwarancji.
3. Wszystkie zaoferowane elementy przedmiotu zamówienia muszą być ze sobą kompatybilne.
4. Dostarczony sprzęt winien mieć preinstalowany system operacyjny
5. Wykonawca w pozycjach, gdzie Zamawiający wymagał witryny/strony producenta może wskazać inną witrynę/stronę na której będą znajdowały się informacje o wskazanym przez Zamawiającego zakresie.
6. W pozycjach, gdzie Zamawiający wymagał podania Producenta, modelu lub nazwy lub typu itp. Zamawiający dopuszcza, aby Wykonawca nie podawał pełnych danych pod warunkiem, iż wskazane w ofercie informacje umożliwiają prawidłową identyfikację zaoferowanego produktu/podzespołu.
* Oświadczamy, że w/w przedmiot zamówienia spełnia wszystkie wymienione w powyższej tabeli wymagania.
* Oświadczamy, że w/w oferowany przedmiot zamówienia jest kompletny i będzie gotowy do użytkowania bez żadnych dodatkowych inwestycji.
* Oświadczamy, iż wszystkie zaoferowane elementy przedmiotu zamówienia są ze sobą kompatybilne.

................................................................................. czytelny podpis i pieczęć osoby uprawnionej/

 osób uprawnionych do reprezentowania Wykonawcy

DZP/381/45B/2019 Załącznik nr 5 do SIWZ (załącznik nr 3 do umowy)

ZESTAWIENIE PARAMETRÓW TECHNICZNYCH

**Pakiet 2: Zestawy komputerowe - typu stojącego T/MT**

3 sztuki, w tym:

dla lokalizacji Ceglana – 2 sztuki,

dla lokalizacji Ligota 1 sztuka

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagania minimalne – parametry techniczne komputerów** | **Faktycznie (oferowane) przez Wykonawcę parametry** |
|  | **Zestaw komputerowy - typu stojącego T/MT** (**Tower/Micro Tower)****Producent, Typ/Model: zgodnie z wypełnionym formularzem asortymentowo cenowym.** |
| 1.  | **Zastosowanie:**  |  |
|  | Komputer wykorzystywany dla potrzeb aplikacji biurowych, bazodanowych, projektowych, czytania dokumentacji technicznych w plikach m.in.: dwg, pdf, a w szczególności systemu InfoMedica/AMMS produkcji Asseco Poland (posiadanym przez Zamawiającego). | TAK / NIE\* |
| 2 | **Procesor:** |  |
|  | Procesor wielordzeniowy przeznaczony do komputerów stacjonarnych stosowanych w rozwiązaniach biznesowych. Musi umożliwiać obsługę zarówno 32-bitowych jak i 64-bitowych aplikacji oraz posiadać sprzętowe wsparcie wirtualizacji. Oferowany procesor ma osiągnąć wydajność min 11900 pkt. w benchmarku PassMark High End CPU’s: znajdującego się na stronie https://www.cpubenchmark.net/high\_end\_cpus.html) - wg załączonego wydruku z dnia 28.05.2019 z stanowiącego załącznik nr 9 do SIWZ)W przypadku zaoferowania procesora, który nie będzie widniał w załączniku nr 9 do SIWZ lub w przypadku użycia przez oferenta innych testów wydajności niż wskazane przez Zamawiającego Wykonawca na wezwanie Zamawiającego na podstawie art. 26 ust 2 lub 3 ustawy PZP będzie zobowiązany złożyć oprogramowanie testujące, testowany zestaw (tj. oferowany przez Wykonawcę sprzęt w ilości 1 szt. do zwrotu Wykonawcy) oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia. .Procesor musi wspierać technologie udostępniania informacji o podzespołach komputera i jego oprogramowaniu, zdalnego dostępu do komputera (monitoring, sterowanie nim, konserwację niezależnie od stanu systemu operacyjnego nawet w gdy komputer jest wyłączony), oraz sprzętowe wsparcie pamięci transakcyjnej. | TAK / NIE\*Podać producenta i typ/model procesora…………………………… |
| 3 | **Płyta główna** |  |
|  | Dedykowana do komputera typu (MT) micro tower (przeznaczona do rozwiązań biznesowych i profesjonalnych). Dostosowana do oferowanego procesora, umożliwiająca obsługę magistrali zainstalowanego procesora, wysokowydajnej pamięci zgodnej z oferowanym procesorem oraz wykorzystanie wszystkich technologii zawartych w oferowanym procesorze. | TAK / NIE\*Podać producenta i typ/model płyty…………………………… |
| 4 | **Pamięć RAM** |  |
|  | Min. 32 GB pamięci RAM w technologii zgodnej z zainstalowanym procesorem z możliwością rozszerzenia do 64GB (co najmniej 2 wolne złącza pamięci RAM) | TAK / NIE\*Podać producenta i typ/model pamięci…………………………… |
| 5 | **Dysk twardy** |  |
|  | Min. 250GB GB w technologii SSD, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego po awarii bez dodatkowych nośników.  | TAK / NIE\*Podać producenta i typ/model dysku …………………………… |
|  | Dodatkowy dysk twardy minimum 1TB, 7200rpm | TAK / NIE\*Podać producenta i typ/model dysku…………………………… |
| 6 | **Karta graficzna** |  |
|  | Z akceleracją 2D/3D. Wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki, możliwość osiągnięcia rozdzielczości 1920x1080 pikseli z maksymalną głębia kolorów 32 bpp. Karta musi zapewniać jednoczesną obsługę dwóch monitorów (każdy w trybie Full HD) dostarczonych wraz z niniejszą jednostką centralną. | TAK / NIE\*Podać producenta i typ/model karty graficznej…………………………… |
| 7 | **Karta dźwiękowa / multimedia** |  |
|  | - Karta dźwiękowa zintegrowana z płytą główną, zgodna z HDA | TAK / NIE\* |
| 8 | **Komunikacja** |  |
|  | - Zintegrowany z płytą główną kontroler LAN Ethernet obsługujący standardy 10/100/1000 Mbits z obsługą VLAN 802.1q- Kontroler WIFI 802.11b/g/n lub 802.11ac z anteną**Żaden z powyższych kontrolerów nie może być podłączony do komputera poprzez złącze USB.** | TAK / NIE\* |
| 9 | **Porty** |  |
|  | Zaoferowany komputer musi posiadać minimum:- 2 x Display Port oraz 1 x HDMI lub 3 x Display Port- 1 x RJ-45- 8 portów USB (w tym co najmniej 4 porty USB 3.1 z przodu ) - 1 x AudioWymagana ilość (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, hubów itp.  | TAK / NIE\* |
| 10 | **Peryferia** |  |
|  | - Klawiatura przewodowa (długość kabla min 1.4 m) USB w układzie polski programisty - Mysz optyczna przewodowa (długość kabla min 1.4 m) USB z rolką, DPI minimum 1600- Czytnik kart 5w1 lub 7w1 – obsługa kart SD, SDHC, MMS, miniSD, SDXC (zamontowany wewnątrz obudowy komputera) | TAK / NIE\* |
| 11 | **Napęd optyczny** |  |
|  | Wbudowana nagrywarka DVD +/-RW | TAK / NIE\* |
| 12 | **Ekran** |  |
|  | Komputer musi być wyposażony w dwa monitory zewnętrzne o poniższych parametrach wraz z niezbędnymi kablami umożliwiającymi jednoczesna prace z komputeremMonitor musi posiadać minimalne parametry:- rozdzielczość FULL HD 1920x1080- przekątna min. 24,5 cala- matryca matowa typu TN LED- 16 mln kolorów- kontrast statyczny 1000:1- czas reakcji matrycy nie większy niż 1ms- jasność wyświetlacza nie mniejsza niż 400cd/m2- funkcja redukcji niebieskiego światła- możliwość regulacji pochylenia w zakresie nie mniejszym niż 25st- możliwość regulacji obrotowej tzw ‘pivot’- maksymalne zużycie energii nie może przekraczać 28W w trybie pracy, a w trybie czuwania nie więcej niż 0,5W- monitor musi posiadać możliwość montażu na ścianie z wykorzystaniem otworów montażowych w standardzie VESA 100, z możliwością bez narzędziowego demontażu stopy | TAK / NIE\***Producent, typ/model monitora – zgodnie z wypełnionym formularzem asortymentowo cenowym**  |
| 13 | **Obudowa** |  |
|  | Obudowa typu MT (micro tower) z obsługą kart PCI Express wyłącznie o pełnym profilu (minimum 2x PCI Express x16, 1x PCI Express x1). Obudowa wyposażona w minimum dwie kieszenie zewnętrzne 5,25” (dopuszcza się zastosowanie jednej kieszenie 5,25” w wersji SLIM dla napędu optycznego) oraz jedną kieszeń 3,5” w której umieszczony będzie czytnik kart, dwie wewnętrzne kieszenie 3,5” i jedną 2,5”. Obudowa musi umożliwiać bez narzędziową wymianę dysków i kart rozszerzających. Obudowa trwale oznaczona nazwą producenta obudowy. Obudowa przystosowana do pracy w pionie, wyposażona w zasilacz z aktywnym korektorem PFC o sprawności energetycznej do 92% (certyfikat 80PLUS Platinium) | TAK / NIE\* |
| 14 | **Zabezpieczenia fizyczne** |  |
|  | Brak wymagań | -------------- |
| 15 | **Zasilanie i eksploatacja** |  |
|  | Urządzenie spełniające wymagania rozporządzenia Komisji (UE) Nr 617/2013 w sprawie wykonania dyrektywy Parlamentu Europejskiego i Rady 2009/125/WE, posiada oznakowanie CE i wydaną deklarację zgodności WE (załącznik VI do dyrektywy 2009/125/WE) | TAK / NIE\* |
| 16 | **System operacyjny** |  |
|  | Zainstalowany system operacyjny wg wymagań wyszczególnionych poniżej, z licencją dożywotnią**Wymagania dla systemu:****DOTYCZY WSZYSTKICH KOMPUTERÓW ( tj. 3 licencji )**Preinstalowany fabrycznie na dysku twardym system operacyjny w polskiej wersji językowej. System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:1. Możliwość pracy w systemie Infomedica/AMMS produkcji Asseco Poland (posiadanym przez Zamawiającego)
2. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek
3. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu
4. Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW
5. Internetowa aktualizacja zapewniona w języku polskim
6. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6
7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe
8. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi)
9. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer
10. Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta
11. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu
12. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników
13. 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
14. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych
15. Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego
16. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika
17. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi
18. Wbudowany system pomocy w języku polskim
19. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących)
20. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji
21. Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny
22. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509
23. Wsparcie dla logowania przy pomocy smartcard
24. Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji
25. System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk
26. Wsparcie dla Java i .NET Framework 1.1 i 2.0 i 3.0 i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach
27. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń
28. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem
29. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację
30. Graficzne środowisko instalacji i konfiguracji
31. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe
32. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
33. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej
34. Możliwość przywracania plików systemowych
35. 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.)

Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu | TAK / NIE\*Podać producenta i nazwę zaoferowanego oprogramowania ……………………………dot. podpunktu 3podać nazwę strony serwera WWW ………………………… |
| 17 | **Pakiet antywirusowy DOTYCZY WSZYSTKICH KOMPUTERÓW DLA LOKALIZACJI CEGLANA ( tj. 2 licencje ). Nie dotyczy lokalizacji Ligota** |  |
|  | Zainstalowany pakiet antywirusowy wg wymagań wyszczególnionych poniżej.* Zamawiający obecnie posiada pakiet antywirusowy ESET Endpoint Security do użytku dla biznesu (**381** licencji w lokalizacji Ceglana ważnych do 5.09.2020r) wraz z wdrożoną konsolą do centralnego zarządzania,
* Użyte przez Zamawiającego wszelkie nazwy handlowe, znaki towarowe, patenty i miejsce pochodzenia są uzasadnione specyfiką przedmiotu zamówienia i mają na celu wskazanie jedynie jakości przedmiotu zamówienia.

***Wymagania ogólne:**** Udzielona licencja powinna umożliwić użytkowanie programu we wszystkich jednostkach organizacyjnych Zamawiającego.
* W przypadku zaoferowania ESET Endpoint Security Suite, zamawiający wymaga, by licencja była dostarczona w formie rozszerzenia klucza dla **381** licencji przytoczonych powyżej, o ilość równą ilości zamawianych komputerów dla lokalizacji Ceglana **tj. 2 licencje z okresem ważności jak posiadany klucz przez Zamawiającego - Identyfikator publiczny 333-99N-HA7**,
* W przypadku zaoferowania innego pakietu antywirusowego niż obecnie posiadany przez Zamawiającego wymaga się, aby współpracował on z konsolą centralnego zarządzania posiadaną i wdrożoną przez Zamawiającego ESET Remote Administrator Console. Poniżej Zamawiający wskazuje wymagania minimalne dla pakietu antywirusowego:

***Wymagania ogólne dla stacji roboczych:*** * Pełne wsparcie dla zaoferowanego systemu operacyjnego
* Wersja programu dostępna w całości w języku polskim
* Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim

***Ochrona antywirusowa i antyspyware:**** Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
* Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
* Wbudowana technologia do ochrony przed rootkitami.
* Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
* Możliwość skanowania całego dysku, dysków sieciowych oraz nośników zewnętrznych wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
* System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak - nie wykonywało danego zadania.
* Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami, (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
* Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
* Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
* Skanowanie plików spakowanych i skompresowanych.
* Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).
* Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
* Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
* Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
* W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
* Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
* Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
* 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).
* Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym.
* Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.
* Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
* Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
* Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.
* Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
* Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
* Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
* Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
* Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
* Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
* Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
* Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
* Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
* W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.
* Wbudowane dwa niezależne moduły heurystyczne - jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej i/lub obu metod jednocześnie.
* Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
* Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
* Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
* Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
* Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
* Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik komputera przy próbie dostępu do konfiguracji był proszony o podanie hasła.
* Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
* Możliwość zabezpieczenia hasłem konfiguracji programu oraz jego nieautoryzowanej próby deinstalacji
* Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji - poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
* Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
* Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
* System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
* Program ma umożliwiać 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
* Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
* Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.
* Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
* W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
* Użytkownik ma posiadać możliwość takiej konfiguracji aplikacji aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
* Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
* Moduł HIPS musi posiadać możliwość pracy w jednym z czterech trybów:
* tryb automatyczny z regułami gdzie aplikacja automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
* tryb interaktywny, w którym to aplikacja 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 aplikacja uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu aplikacja musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
* Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
* Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
* Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
* Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
* Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
* Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
* Aplikacja musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
* Aplikacja musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http
* Aplikacja musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
* Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
* Program ma wspierać technologię CISCO NetWork Access Control.
* Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
* W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór następujących modułów do instalacji: ochrona antywirusowa i antyspywerowa, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, kopia dystrybucyjna

***Ochrona przed spamem:*** * Ochrona antyspamowa dla różnych programów pocztowych wykorzystująca filtry Bayes-a, białą i czarną listę oraz bazę charakterystyk wiadomości spamowych.
* Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
* Integracja z różnymi programami pocztowymi - antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego.
* Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
* Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym.
* Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam.
* Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam.
* Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana” oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana”.
* Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

***Zapora osobista (personal firewall):*** * Zapora osobista ma pracować jednym z 5 trybów:
* tryb automatyczny - program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące,
* tryb automatyczny z wyjątkami - działa podobnie jak tryb automatyczny, ale umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł,
* tryb interaktywny - program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo),
* tryb oparty na regułach - użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany,
* tryb uczenia się - umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji.
* Możliwość tworzenia list sieci zaufanych.
* Możliwość dezaktywacji funkcji zapory sieciowej na kilka sposobów: pełna dezaktywacja wszystkich funkcji analizy ruchu sieciowego, tylko skanowanie chronionych protokołów oraz dezaktywacja do czasu ponownego uruchomienia komputera.
* Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
* Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję.
* Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń.
* Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.
* Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.
* Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
* Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.
* Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
* Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
* Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci
* Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
* Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, aktywności wyłącznie jednego połączenia sieciowego lub wielu połączeń sieciowych konkretny interfejs sieciowy w systemie.
* Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6
* Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci.
* Możliwość aktualizacji sterowników zapory osobistej po restarcie komputera.

***Kontrola dostępu do stron internetowych:**** Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.
* Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
* Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
* Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
* Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i pod kategorii.
* Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
* Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta.
* Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.
 | TAK / NIE\*Podać producenta i nazwę zaoferowanego oprogramowania …………………………… |
| 18 | **Pakiet biurowy** |  |
|  | Zainstalowany pakiet biurowy wg wymagań wyszczególnionych poniżej z licencją dożywotnią.***Wymagania ogólne:*** * Licencja pakietu oprogramowania biurowego typu MS Office Home and Business 2016/2019 PL lub równoważne wg wskazania poniżej
* Pełne wsparcie dla zaoferowanego systemu operacyjnego
* Wymagania odnośnie interfejsu użytkownika:
* Pełna polska wersja językowa interfejsu użytkownika.
* Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
* - Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – 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.
* Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim

***Definicja równoważności dla pakietu oprogramowania biurowego:**** Zamawiający uzna pakiet oprogramowania biurowego za równoważny określonemu w SIWZ, gdy spełni poniższe wymagania:
* Oprogramowanie biurowe w najnowszej dostępnej na rynku wersji.
* Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu.
* Wymagane jest prawo do instalacji aktualizacji i poprawek do danej wersji oprogramowania, udostępnianych bezpłatnie przez producenta na jego stronie internetowej w okresie co najmniej 5 lat.
* Zamawiający wymaga, aby wszystkie elementy oprogramowania biurowego oraz jego licencja pochodziły od tego samego producenta.
* Zawierające w pakiecie przynajmniej edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji. Aplikacja do tworzenia prezentacji powinna umożliwiać udostępnianie prezentacji przy użyciu przeglądarki internetowej bez potrzeby instalowania dodatkowych elementów ani konfigurowania. Do każdej prezentacji można dodać wciągające wideo, aby zwrócić uwagę odbiorców. Nagrania wideo można wstawiać bezpośrednio w programie, a następnie dostosowywać je, przycinać lub oznaczać najważniejsze sceny w nagraniu zakładkami, aby zwrócić na nie szczególną uwagę. Wstawiane nagrania są domyślnie osadzone, dzięki czemu nie trzeba zarządzać dodatkowymi plikami wideo. Pliki programów edytora tekstów, arkusza kalkulacyjnego i programu do tworzenia prezentacji można przechowywać online i uzyskiwać do nich dostęp, przeglądać, edytować i udostępniać innym użytkownikom.

***Pakiet biurowy musi spełniać następujące wymagania:*** * Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
* posiada kompletny i publicznie dostępny opis formatu,
* ma zdefiniowany układ informacji w postaci XML zgodnie z rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U 2017 poz. 2247),
* umożliwia wykorzystanie schematów XML,
* wspiera w swojej specyfikacji podpis elektroniczny zgodnie z rozporządzeniem Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U 2017 poz. 2247),
* 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 makropoleceń, język skryptowy).
* Pakiet zintegrowanych aplikacji biurowych musi zawierać:
* Edytor tekstów.
* Arkusz kalkulacyjny.
* Narzędzie do przygotowywania i prowadzenia prezentacji.
* Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).
* Edytor tekstów musi umożliwiać:
* 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.
* Automatyczne tworzenie spisów treści.
* Formatowanie nagłówków i stopek stron.
* Sprawdzanie pisowni w języku polskim.
* Śledzenie zmian wprowadzonych przez użytkowników.
* Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
* Określenie układu strony (pionowa/pozioma).
* Wydruk dokumentów.
* Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
* Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
* Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
* 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.
* 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.
* 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.
	+ Arkusz kalkulacyjny musi umożliwiać:
* Tworzenie raportów tabelarycznych.
* Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.
* 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.
* Wyszukiwanie i zamianę danych.
* Wykonywanie analiz danych przy użyciu formatowania warunkowego.
* 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.
* Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
* Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
	+ Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
	+ Przygotowywanie prezentacji multimedialnych.
	+ 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.
	+ Umieszczanie 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.
	+ Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.
	+ Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
	+ Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.
	+ Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.
	+ Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.
	+ Automatyczne grupowanie poczty o tym samym tytule.
	+ Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.
	+ Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia.
	+ Zarządzanie kalendarzem.
	+ Udostępnianie kalendarza innym użytkownikom.
	+ Przeglądanie kalendarza innych użytkowników.
	+ Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.
	+ Zarządzanie listą zadań.
	+ Zlecanie zadań innym użytkownikom.
	+ Zarządzanie listą kontaktów.
	+ Udostępnianie listy kontaktów innym użytkownikom.
	+ Przeglądanie listy kontaktów innych użytkowników.
	+ Możliwość przesyłania kontaktów innym użytkowników.
 | TAK / NIE\***Podać producenta i nazwę zaoferowanego oprogramowania** **……………………………………………………………………………………………………………………..** |
| 18 | **Gwarancja** |  |
|  | **Komputer musi posiadać pakiet serwisowy oferujący następujące warunki gwarancji:**- Gwarancja min. 36 miesięcy na części i czynności serwisowe (gwarancja na miejscu u klienta z czasem reakcji do końca następnego dnia roboczego od zgłoszenia)- Czas usunięcia awarii w okresie gwarancji max 14 dni roboczych (zgodnie z zadeklarowanym terminem w formularzu ofertowym) od momentu pisemnego zgłoszenia awarii, sprzęt do naprawy i z naprawy Wykonawca dostarcza na swój koszt, W przypadku awarii dysku twardego lub komputera dysk pozostaje u Zamawiającego- Komputer nie będzie posiadał plomb lub innych elementów ograniczających dostęp do wnętrza- Firma serwisująca musi być autoryzowanym serwisem producenta komputera- Wykonawca zobowiązany jest do wskazania danych kontaktowych do zgłaszania awarii sprzętu - Możliwość pobierania dokumentacji i sterowników z jednej lokalizacji w sieci Internet- Możliwość uzyskania pomocy technicznej producenta w języku polskim za pomocą strony WWW, telefonicznie np. infolinii itp.- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera- Możliwość weryfikacji czasu obowiązywania gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera | TAK / NIE\*Uzupełnić:……….. miesięcy na miejscu u klienta z czasem reakcji do końca następnego dnia roboczego od zgłoszeniaUzupełnić:Dane kontaktowe do zgłaszania awarii:………………………..………………………..………………………..Dane kontaktowe do weryfikacji czasu obowiązywania gwarancji:………………………..………………………..……………………….. |
| 19 | **Inne, ergonomia** |  |
|  | - Produkt musi być fabrycznie nowy. Niedozwolone jest oferowanie sprzętu z programów Refurbished itp.- Kabel zasilający | TAK / NIE\* |

 **\* niewłaściwe skreślić lub właściwe zaznaczyć**

1. W kolumnie „Faktyczne (oferowane przez Wykonawcę) parametry” w pozycjach TAK/NIE\* zaznaczanie odpowiedzi NIE oznacza niespełnienie wymaganych przez Zamawiającego parametrów.
2. Zamawiający zastrzega sobie możliwość rozbudowy komputera, bez powiadomienia o tym Wykonawcy bez utraty gwarancji.
3. Wszystkie zaoferowane elementy przedmiotu zamówienia muszą być ze sobą kompatybilne.
4. Dostarczony sprzęt winien mieć preinstalowany system operacyjny o
5. Wykonawca w pozycjach, gdzie Zamawiający wymagał witryny/strony producenta może wskazać inną witrynę/stronę na której będą znajdowały się informacje o wskazanym przez Zamawiającego zakresie.
6. W pozycjach, gdzie Zamawiający wymagał podania Producenta, modelu lub nazwy lub typu itp. Zamawiający dopuszcza, aby Wykonawca nie podawał pełnych danych pod warunkiem, iż wskazane w ofercie informacje umożliwiają prawidłową identyfikację zaoferowanego produktu/podzespołu.
* Oświadczamy, że w/w przedmiot zamówienia spełnia wszystkie wymienione w powyższej tabeli wymagania.
* Oświadczamy, że w/w oferowany przedmiot zamówienia jest kompletny i będzie gotowy do użytkowania bez żadnych dodatkowych inwestycji.
* Oświadczamy, iż wszystkie zaoferowane elementy przedmiotu zamówienia są ze sobą kompatybilne.

.................................................................................

 czytelny podpis i pieczęć osoby uprawnionej/

 osób uprawnionych do reprezentowania Wykonawcy

DZP/381/45B/2019 Załącznik nr 5 do SIWZ (załącznik nr 3 do umowy)

ZESTAWIENIE PARAMETRÓW TECHNICZNYCH

**PAKIET 3 – DRUKARKI LASEROWE**

30 sztuk, w tym:

dla lokalizacji Ceglana – 10 sztuk,

dla lokalizacji Ligota – 20 sztuk

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagania minimalne – parametry techniczne drukarek** | **Faktycznie (oferowane) przez Wykonawcę parametry** |
|  | **DRUKARKA LASEROWA****Producent, Typ/Model: zgodnie z wypełnionym formularzem asortymentowo cenowym.** |
| 1 | **Zastosowanie:** |
|  | Drukarki wykorzystywane dla potrzeb aplikacji biurowych, a w szczególności systemu InfoMedica/AMMS produkcji Asseco Poland (posiadanym przez Zamawiającego). | TAK / NIE\* |
| 2 | **Pamięć:** |  |
|  | Min. 512 MB RAM | TAK / NIE\* |
| 3 | **Formaty papieru:** |  |
|  | Podajnik 1: A4, A5, B5(JIS), A6, Letter, Legal 13, Legal 14, Executive, StatementPodajnik wielofunkcyjny: A4, A5, B5(JIS), A6, Letter, Legal 13, Legal 14, Executive, Statement, koperty (Monarch, 9, 10, DL, C5, C6), Formaty niestandardowe (do 1321 mm długości łącznie ze wstęgami), 4 × 6”, 5 × 7” Tryb dwustronny: A4, B5(JIS), Letter, do Legal 14, Executive | TAK / NIE\* |
| 4 | **Czas do uzyskania pierwszej kopii // Prędkość wydruku** |  |
|  | Maks 7 sekund // minimum 40 str./min. | TAK / NIE\* |
| 5 | **Czas nagrzewania** |  |
|  | maks 15,0 s od momentu włączenia | TAK / NIE\* |
| 6 | **Rozdzielczość** |  |
|  | Min 600 x 600 dpi | TAK / NIE\* |
| 7 | **Duplex** |  |
|  | Tak, zainstalowany automatyczny | TAK / NIE\* |
| 8 | **Podajniki papieru** |  |
|  | Podajnik 1: maks. 250 arkuszy 80 g/m2Podajnik wielofunkcyjny: maks. 100 arkuszy 80 g/m2 | TAK / NIE\* |
| 9 | **Materiały eksploatacyjne** |  |
|  | Możliwość instalacji tonera o wydajności minimum 10000 stron wg ISO/IEC 19752/19798 | TAK / NIE\* |
|  | Urządzenie wyposażone w startowy toner producenta urządzenia o wydajności minimum 2000 stron wg ISO/IEC 19752/19798 | TAK / NIE\* |
| 10 | **Maksymalna pojemność podajników** |  |
|  | Min. 500 arkuszy (włącznie z podajnikami opcjonalnymi) | TAK / NIE\* |
| 11 | **Czcionki drukarki** |  |
|  | Emulacja PostScript – min. 130 czcionekemulacja PCL – min. 80 | TAK / NIE\* |
| 12 | **Komunikacja** |  |
|  | - Ethernet 10/100/1000- USB 2.0 | TAK / NIE\* |
| 13 | **Języki drukarki** |  |
|  | PostScript, emulacja PCL 5e, emulacja PCL 6 (XL), emulacja PDF v1.7 | TAK / NIE\* |
| 14 | **Sieć i protokoły** |  |
|  | Wszystkie główne protokoły sieciowe za pośrednictwem karty sieciowej Ethernet z wewnętrznym serwerem WWW do konfigurowania drukarki i karty sieciowej oraz zarządzania nimi. TCP/IPv4/v6, NetBIOS przez TCP, DHCP, BOOTP, HTTP, HTTPS, DNS, UPnP, Bonjour, SMTP, POP3, SNMPv1/v3, SNTP, IPP, IPPS, LPR, Port9100 | TAK / NIE\* |
| 15 | **Zasilanie** |  |
|  | 230 VAC +/- 10%, 50 lub 60 Hz +/-2% | TAK / NIE\* |
| 16 | **Pobór mocy** |  |
|  | Tryb pracy: maks. 900 WTryb drukowanie: maks. 650 WTryb gotowości: maks. 10 WTryb oszczędzania energii: < 5 WTryb głębokiego uśpienia: < 2 WAutomatyczne wyłączanie: < 0,5 W | TAK / NIE\* |
| 17 | **Poziom hałasu / ciśnienie akustyczne** |  |
|  | Podczas pracy: maks 55 dB(A)Tryb czuwania: maks 38 dB(A) | TAK / NIE\* |
| 18 | **Obciążalność** |  |
|  | Minimalnie: 50 000 stron/miesiąc | TAK / NIE\* |
| 19 | **Warunki gwarancyjne:** |  |
|  | Minimum 36 miesięcy na urządzenie w miejscu instalacji, od momentu podpisania protokołu dostawy do Zamawiającego | TAK / NIE\*Uzupełnić:……….. miesięcy na urządzenie w miejscu instalacji, od momentu podpisania protokołu dostawy do Zamawiającego |
|  | Serwis urządzenia musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta | TAK / NIE\* |
|  | Czas usunięcia awarii max. 14 dni roboczych od momentu pisemnego zgłoszenia awarii, sprzęt do naprawy i z naprawy Wykonawca dostarcza na swój koszt | TAK / NIE\* |
| 20 | **Wymagania ogólne:** |  |
|  | Dostarczony sprzęt musi być fabrycznie nowy. Niedozwolone jest oferowanie sprzętu z programów Refurbished itp. | TAK / NIE\* |

1. W kolumnie „Faktyczne (oferowane przez Wykonawcę) parametry” w pozycjach TAK/NIE\* zaznaczanie odpowiedzi NIE oznacza niespełnienie wymaganych przez Zamawiającego parametrów.
2. Wszystkie zaoferowane elementy przedmiotu zamówienia muszą być ze sobą kompatybilne.
* Oświadczamy, że w/w oferowany przedmiot zamówienia jest kompletny i będzie gotowy do użytkowania bez żadnych dodatkowych inwestycji.
* Oświadczamy, iż wszystkie zaoferowane elementy przedmiotu zamówienia są ze sobą kompatybilne.

................................................................................. czytelny podpis i pieczęć osoby uprawnionej/

 osób uprawnionych do reprezentowania Wykonawcy

DZP/381/45B/2019 Załącznik nr 5 do SIWZ (załącznik nr 3 do umowy)

ZESTAWIENIE PARAMETRÓW TECHNICZNYCH

**PAKIET 4 – DRUKARKI ETYKIET I CZYTNIKI KODÓW KRESKOWYCH**

Pozycja 1 Drukarki etykiet - 2 sztuki dla lokalizacji Ceglana

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagania minimalne – parametry techniczne drukarek** | **Faktycznie (oferowane) przez Wykonawcę parametry** |
|  | **DRUKARKA ETYKIET** **Producent, Typ/Model: zgodnie z wypełnionym formularzem asortymentowo cenowym.** |
| 1 | **Zastosowanie:** |
|  | Drukarki wykorzystywane dla potrzeb wykorzystywanej przez Zamawiającego aplikacji medycznej AMMS firmy ASSECO S.A. do znakowania dokumentacji medycznej | TAK / NIE\* |
| 2 | **Pamięć:** |  |
|  | Min. 8 MB SDRAM i min. 4MB Flash | TAK / NIE\* |
| 3 | **Rodzaj wydruku:** |  |
|  | Minimum termo-transferowy | TAK / NIE\* |
| 4 | **Parametry techniczne:** |  |
|  | * Rozdzielczość minimum 8 pkt/mm (203 dpi)
* Maksymalna szerokość druku 104mm
* Maksymalna długość druku 990mm
 | TAK / NIE\* |
| 5 | **Języki drukarki:** |  |
|  | Minimum EPL, ZPL | TAK / NIE\* |
|  | 1D: minimum Code 39, Code 128, Code 93, Codabar/NW7, Code 11, UPC/EAN | TAK / NIE\* |
|  | 2D: minimum PDF417, DataMatrix, MaxiCode, QR Code | TAK / NIE\* |
| 6 | **Komunikacja:** |  |
|  | - szeregowy RS232- Ethernet 10/100Mbit- USB 2.0 | TAK / NIE\* |
| 7 | **Zasilanie:** |  |
|  | 230 VAC +/- 10%, 50 lub 60 Hz +/-2% | TAK / NIE\* |
| 8 | **Warunki gwarancyjne:** |  |
|  | Minimum 36 miesięcy na urządzenie wraz z głowicą od momentu podpisania protokołu dostawy do Zamawiającego | TAK / NIE\*Uzupełnić:……….. miesięcy na urządzenie wraz z głowicą od momentu podpisania protokołu dostawy do Zamawiającego |
|  | Serwis urządzenia musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta | TAK / NIE\* |
|  | Czas usunięcia awarii max. 14 dni roboczych od momentu pisemnego zgłoszenia awarii, sprzęt do naprawy i z naprawy Wykonawca dostarcza na swój koszt | TAK / NIE\* |
| 9 | **Wymagania ogólne:** |  |
|  | Dostarczony sprzęt musi być fabrycznie nowy. Niedozwolone jest oferowanie sprzętu z programów Refurbished itp. | TAK / NIE\* |
|  |

**\* niewłaściwe skreślić lub właściwe zaznaczyć**

Pozycja 2: Czytniki Kodów Kreskowych 2 sztuki dla lokalizacji Ligota

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagania minimalne – parametry techniczne drukarek** | **Faktycznie (oferowane) przez Wykonawcę parametry** |
|  | **CZYTNIK kodów kreskowych****Producent, Typ/Model: zgodnie z wypełnionym formularzem asortymentowo cenowym.** |
| 1 | **Zastosowanie:** |
|  | Czytniki będą wykorzystywane do skanowania dwuwymiarowych kodów QR Code oraz DataMatrix współpracując z posiadanym przez Zamawiającego systemem AMMS firmy ASSECO S.A. | TAK / NIE\* |
| 2 | **Odczytywane kody:** |  |
|  | 1D: minimum Code 39, Code 128, Code 93, Codabar/NW7, Code 11, UPC/EAN | TAK / NIE\* |
|  | 2D: minimum PDF417, TLC-39, DataMatrix, MaxiCode, QR Code, MicroQR, kody złożone, kody pocztowe | TAK / NIE\* |
| 3 | **Interfejsy komunikacyjne:** |  |
|  | Minimum USB, RS232, Keyboard Wedge (złącze klawiatury) | TAK / NIE\* |
| 4 | **Wskaźniki dla użytkownika:** |  |
|  | Bezpośredni wskaźnik odczytu, wskaźnik LED dobrego odczytu, sygnał dźwiękowy | TAK / NIE\* |
| 5 | **Źródło światła:** |  |
|  | Wzór celujący liniowy | TAK / NIE\* |
| 6 | **Czujnik obrazu:** | TAK / NIE\* |
|  | Minimum 640 x 480 pikseli | TAK / NIE\* |
| 7 | **Tryb pracy:** |  |
|  | Bezprzewodowy | TAK / NIE\* |
| 8 | **Odporność na upadki:** |  |
|  | Konstrukcja odporna na wielokrotne upadki na beton z wysokości 1,5m | TAK / NIE\* |
| 9 | **Klasa szczelności:** |  |
|  | Minimum IP42 | TAK / NIE\* |
| 10 | **Łączność pomiędzy stacją dokującą a czytnikiem:** |  |
|  | Zapewniająca prawidłową prace czytnika w odległości do 10m od stacji dokującej | TAK / NIE\* |
| 11 | **Bateria:** |  |
|  | Zapewniająca pracę po pełnym naładowaniu na minimum 12h | TAK / NIE\* |
| 12 | **Bezpieczeństwo:** |  |
|  | Parametry środowiskowe: RoHS EN 50581 lub nowsza | TAK / NIE\* |
|  | Bezpieczeństwo diod LED: IEC 62471 lub nowsza | TAK / NIE\* |
| 13 | **Akcesoria:** |  |
|  | Stacja do obsługi automatycznej, zapasowa bateria, kabel micro USB do podłączenia z komputerem | TAK / NIE\* |
| 14 | **Warunki gwarancyjne:** |  |
|  | Minimum 36 miesięcy na urządzenie od momentu podpisania protokołu dostawy do Zamawiającego | Uzupełnić:……….. miesięcy  |
|  | Serwis urządzenia musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta | TAK / NIE\* |
|  | Czas usunięcia awarii max. 14 dni roboczych od momentu pisemnego zgłoszenia awarii, sprzęt do naprawy i z naprawy Wykonawca dostarcza na swój koszt | TAK / NIE\* |
| 15 | **Wymagania ogólne:** |  |
|  | Dostarczony sprzęt musi być fabrycznie nowy. Niedozwolone jest oferowanie sprzętu z programów Refurbished itp. | TAK / NIE\* |
|  |

**\* niewłaściwe skreślić lub właściwe zaznaczyć**

UWAGA (dotyczy pozycji 1 i 2)

1. W kolumnie „Faktyczne (oferowane przez Wykonawcę) parametry” w pozycjach TAK/NIE\* zaznaczanie odpowiedzi NIE oznacza niespełnienie wymaganych przez Zamawiającego parametrów.
2. Wszystkie zaoferowane elementy przedmiotu zamówienia muszą być ze sobą kompatybilne.
* Oświadczamy, że w/w oferowany przedmiot zamówienia jest kompletny i będzie gotowy do użytkowania bez żadnych dodatkowych inwestycji.
* Oświadczamy, iż wszystkie zaoferowane elementy przedmiotu zamówienia są ze sobą kompatybilne.

................................................................................. czytelny podpis i pieczęć osoby uprawnionej/

 osób uprawnionych do reprezentowania Wykonawcy

DZP/381/45B/2019 Załącznik nr 5 do SIWZ (załącznik nr 3 do umowy)

ZESTAWIENIE PARAMETRÓW TECHNICZNYCH

**PAKIET 5 – Rozbudowa serwera Lenovo x3550 M5**

*W CAŁOŚCI DO LOKALIZACJI CEGLANA*

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagania minimalne – parametry techniczne** | **Faktycznie (oferowane) przez Wykonawcę parametry** |
|  | **Rozbudowa serwera Lenovo x3550 M5 (MT: 8869AC1)**Na prośbę Oferenta/Wykonawcy - Zamawiający może udostępnić NR seryjny urządzenia |
| 1 | **Zastosowanie:** |
|  | Rozbudowa posiadanego przez Zamawiającego serwera Lenovo x3550 M5 o dodatkowe miejsce dyskowe oraz redundantną komunikację z posiadana macierzą | ---------------------------------------- |
| 2 | **Podzespoły:** |  |
|  | Wymagana jest rozbudowa o drugi kontroler HBA o parametrach nie gorszych niż posiadany N2225 HBA 9300-8e PCIe x8 SAS. Kontroler musi dać się zamontować w slocie PCIe poziomo w obudowie serwera (serwer 1U). Kontroler musi posiadać dwa wyjścia zewnętrzne do połączenia z macierzą Storwize v5020 posiadaną przez Zamawiającego dwoma kablami mini SAS HD to mini SAS HD – 1,5 [Zamawiający obecnie posiada part numer 00AR311] które to Wykonawca dostarczy wraz z kontrolerem | TAK / NIE\*Podać part numery części:………………………….………………………….…………………………. |
|  | Rozbudowa o cztery układy pamięci RAM DDR 2133MHz 1.2V CRC 16GB [Zamawiający obecnie posiada part numer 21119E92] | TAK / NIE\* Podać part numer części:…………………………. |
|  | Rozbudowa o trzy dyski twarde Hot-Swap 2,5”, o pojemności 300GB, prędkości obrotowej 10000rpm, interfejsie komunikacyjnym SAS 12Gbps, [Zamawiający obecnie posiada part numer 00WG686]  | TAK / NIE\* Podać part numer części:…………………………. |
| 3 | **Gwarancja** |  |
|  | Gwarancja na podzespoły nie może być krótsza niż 12 miesięcy od daty dostawy | TAK / NIE\*Uzupełnić:..……………… miesięcy od daty dostawy |
|  | Czas usunięcia awarii max. 14 dni roboczych (zgodnie z zadeklarowanym terminem w formularzu ofertowym od momentu pisemnego zgłoszenia awarii, sprzęt do naprawy i z naprawy Wykonawca dostarcza na swój koszt | TAK / NIE\* |
| 4 | **Pozostałe** |  |
|  | Elementy muszą być produktami producenta serwera posiadanego przez Zamawiającego lub być przez niego certyfikowane | TAK / NIE\* |
|  | W przypadku uszkodzenia pamięci masowej (dysku/ów) uszkodzona pozostaje własnością Zamawiającego | TAK / NIE\* |

**\* niewłaściwe skreślić lub właściwe zaznaczyć**

DZP/381/45B/2019 Załącznik nr 5 do SIWZ (załącznik nr 3 do umowy)

ZESTAWIENIE PARAMETRÓW TECHNICZNYCH

**PAKIET 6 – Rozbudowa serwera NAS Synology RS815**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagania minimalne – parametry techniczne** | **Faktycznie (oferowane) przez Wykonawcę parametry** |
|  | **Rozbudowa serwera NAS Synology RS815+**Na prośbę Oferenta/Wykonawcy - Zamawiający może udostępnić NR seryjny urządzenia |
| 1 | **Zastosowanie:** |
|  | Rozbudowa posiadanego przez Zamawiającego serwera NAS Synology RS815+ dodatkowe zasoby dyskowe oraz drugi serwer NAS umożliwiający utworzenie klastra wysokiej dostępności (HA) z posiadanym serwerem NAS Synology RS815+ | ---------------------------------------- |
| 2 | **Dodatkowe Zasoby Dyskowe :** |  |
|  | Rozbudowa o kompatybilną jednostkę rozszerzającą spełniającą minimalne wymagania:- w 100% kompatybilna z posiadanym serwerem RS815+- 4 kieszenie na dyski twarde- obsługa dysków 3,5” SATA HDD, 2,5” SATA HDD, 2,5” SATA SSD- maksymalna pojemność wewnętrzna 40TB (10TB HDD x 4szt) - obsługa dysków w trybie hot-swap (z możliwością wymiany podczas pracy)- zarządzanie macierzami RAID za pomocą systemu Synology DSM- jeden port zewnętrzny eSATA- obudowa 19” do montażu w szafie krosowej wraz z szynami potrzebnymi do montażu- przywracanie zasilania synchronizowane z serwerem Synology RackStation- wbudowany zasilacz- zakres temperatur pracy urządzenia od 5stC do 35stC- zgodność z dyrektywą RoHS- wyposażona we wszystkie niezbędne akcesoria umożliwiające podłączenie do posiadanego serwera RS815+ oraz montażu w szafie krosowej stojącej 42U 19” | TAK / NIE\*Podać oznaczenie/model:…………………………. |
|  | Wyposażenie dostarczanej jednostki w pięć dysków twardych 3,5” o pojemności min. 6TB (z czego jeden będzie jako zapasowy), prędkości obrotowej min. 7200rpm, interfejsie komunikacyjnym SATA III. 6Gbps, pamięć podręczna min. 64MB, szybkość transmisji SATA min. 600 MB/s, przeznaczenie do serwerów, wyposażone w wieloosiowy czujnik wstrząsów, wykorzystujące technologię zapewniającą integrację, doskonałą ochronę danych oraz optymalną wydajność systemów pracujących w wymagających środowiskach NAS | TAK / NIE\*Podać oznaczenie dysków:…………………………. |
| 3. | **Dodatkowy Serwer NAS na potrzeby klastra HA** |  |
|  | Kompatybilna z posiadanym serwerem NAS Synology jednostka spełniającą minimalne wymagania:- w 100% kompatybilna z posiadanym serwerem RS815+ (używany ten sam system operacyjny)- 4 kieszenie na dyski twarde- pamięć operacyjna minimum 4GB- obsługa dysków 3,5” SATA HDD, 2,5” SATA HDD, 2,5” SATA SSD- obsługa dysków w trybie hot-swap (z możliwością wymiany podczas pracy)- obsługa SMART dla dysków twardych, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów- zarządzanie macierzami RAID za pomocą systemu Synology DSM- jeden port zewnętrzny eSATA- 4 porty Ethernet 1Gbit każdy, wsparcie dla Link Agregation, Jumbo Frame- język GUI: przynajmniej polski i angielski- obudowa 19” nie więcej niż 1U do montażu w szafie krosowej wraz z szynami potrzebnymi do montażu- wbudowane zasilacze (dwa)- zakres temperatur pracy urządzenia od 5stC do 35stC- zgodność z dyrektywą RoHS- wyposażona we wszystkie niezbędne akcesoria umożliwiające montaż w szafie krosowej stojącej 42U 19” | TAK / NIE\*Podać oznaczenie/model:…………………………. |
|  | Dostarczony serwer NAS będzie elementem pasywnym klastra HA, utworzonego za pomocą oprogramowania High Avability Manager, dostępnego na posiadanym przez Zamawiającego serwerze NAS.  | TAK / NIE\* |
|  | Wyposażenie dostarczanej jednostki głównej w pięć dysków twardych 3,5” o pojemności min. 6TB, prędkości obrotowej min. 7200rpm (dwa z nich pozostaną jako zapasowe), interfejsie komunikacyjnym SATA III 6Gbps, pamięć podręczna min. 64MB, szybkość transmisji SATA min. 600 MB/s, przeznaczenie do serwerów, wyposażone w wieloosiowy czujnik wstrząsów, wykorzystujące technologię zapewniającą integrację, doskonałą ochronę danych oraz optymalną wydajność systemów pracujących w wymagających środowiskach NAS | TAK / NIE\*Podać oznaczenie dysków:…………………………. |
| 4. | **Gwarancja** |  |
|  | Gwarancja na jednostkę rozszerzającą oraz dyski twarde nie może być krótsza niż 36 miesięcy od daty dostawy | TAK / NIE\*Uzupełnić:..……………… miesięcy |
|  | Czas usunięcia awarii max. 14 dni roboczych (zgodnie z zadeklarowanym terminem w formularzu ofertowym od momentu pisemnego zgłoszenia awarii, sprzęt do naprawy i z naprawy Wykonawca dostarcza na swój koszt | TAK / NIE\* |
| 5 | **Pozostałe** |  |
|  | Dostarczony sprzęt musi być fabrycznie nowy oraz kompatybilny z posiadanym przez Zamawiającego serwerem | TAK / NIE\* |
|  | W przypadku uszkodzenia urządzenia i konieczności zabrania go do naprawy poza siedzibę Zamawiającego, dyski pozostają u Zamawiającego | TAK / NIE\* |

**\* niewłaściwe skreślić lub właściwe zaznaczyć**

UWAGA:

1. W kolumnie „Faktyczne (oferowane przez Wykonawcę) parametry” w pozycjach TAK/NIE\* zaznaczanie odpowiedzi NIE oznacza niespełnienie wymaganych przez Zamawiającego parametrów.
2. Wszystkie zaoferowane elementy przedmiotu zamówienia muszą być ze sobą kompatybilne oraz kompatybilne z rozbudowywanym serwerem
* Oświadczamy, iż wszystkie zaoferowane elementy przedmiotu zamówienia są ze sobą kompatybilne oraz kompatybilne z rozbudowywanym serwerem

................................................................................. czytelny podpis i pieczęć osoby uprawnionej/

 osób uprawnionych do reprezentowania Wykonawcy

DZP/381/45B/2019 Załącznik nr 5 do SIWZ (załącznik nr 3 do umowy)

ZESTAWIENIE PARAMETRÓW TECHNICZNYCH

**Pakiet 7: Rozbudowa macierzy Lenovo Storwize v5020**

*W CAŁOŚCI DO LOKALIZACJI CEGLANA*

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagania minimalne – parametry techniczne** | **Faktycznie (oferowane) przez Wykonawcę parametry** |
|  | **Rozbudowa macierzy Lenovo Storwize v5020 (MT: 2078-12F )**Na prośbę Oferenta/Wykonawcy - Zamawiający może udostępnić NR seryjny urządzenia |
| 1 | **Zastosowanie:** |
|  | Rozbudowa posiadanej macierzy Lenovo Storwize v5020  | ----------------------------------- |
| 2 | **Rozbudowa o dodatkową półkę dyskową :** |  |
|  | Wymagana jest rozbudowa o drugą półkę dyskową Storwize v5020 expansion MT 2078- wraz z dwunastoma dyskami twardymi Hot-Swap 3,5”, o pojemności minimum 4TB, prędkości obrotowej 7200rpm, interfejsie komunikacyjnym SAS 12Gbps, (Zamawiający obecnie posiada part numer 01AC60) oraz kablami mini SAS HD to mini SAS HD – 1,5 [Zamawiający obecnie posiada part numer 00AR311] koniecznymi do połączenia półki z pierwszą półką posiadaną przez Zamawiającego lub z macierzą – zgodnie z zaleceniami producenta sprzętu. Półka z dyskami do użycia jako rozszerzenie pojemności użytkowej w macierzy.Zamawiający dopuszcza rozwiązanie równoważne tj. nową macierz dyskową o parametrach nie gorszych od posiadanej macierzy Lenovo Storwize v5020, jednocześnie zaproponowana macierz musi spełniać poniższe wymagania:- możliwość montażu jednocześnie minimum 24 dysków 2.5” w jednostce podstawowej,- możliwość podpięcia dodatkowej półki dyskowej rozszerzającej przestrzeń dyskową,- macierz musi zostać wyposażona w minimum 8 dysków 2.5” NL SAS 7.2k 12GB/s o pojemności 2TB każdy,- macierz musi zostać wyposażona w minimum 2 kable przyłączeniowe o długości 2m każdy mini SAS HD to mini SAS HD 12GB/s,- macierz musi posiadać dwa zasilacze redundantne w trybie hot-plug,- macierz musi posiadać obsługę RAID w trybach 0,1,5, 6, 10, 50, 60,- macierz musi posiadać dwa kontrolery SAS wyposażone w minimum 4 porty mini SAS HD na kontroler,- gwarancję min. 5 lat w trybie Next Business Day,- gwarancję na zachowanie dysków twardych przez Zamawiającego w przypadku ich awarii przez cały okres trwania gwarancji | DRUGA PÓLKA DYSKOWA MT 2078-12F /NOWA MACIERZ\***W przypadku zaoferowania półki dyskowej MT 2078-12F:** Podać part numery części:………………………….………………………….………………………….**W przypadku zaoferowania nowej macierzy uzupełnić:** Podać producenta, model i wyposażenie nowej macierzy ………………………….………………………….…………………………. |
| 3 | **Rozbudowa posiadanej półki dyskowej o dodatkowe dyski twarde** |  |
|  | Wymagana jest rozbudowa o jeden dysk twardy Hot-Swap 3,5”, o pojemności min. 300GB, prędkości obrotowej min. 15000rpm, interfejsie komunikacyjnym SAS 12Gbps, (Zamawiający obecnie posiada part numer 01EJ188). Dysk do użycia jako HotSpare dla posiadanych już dysków w macierzy. | TAK / NIE\*Podać part numer części:…………………………. |
|  | Wymagana jest rozbudowa o dziewięć dysków twardy Hot-Swap 3,5”, o pojemności minimum 4TB, prędkości obrotowej 7200rpm, interfejsie komunikacyjnym SAS 12Gbps, [Zamawiający obecnie posiada part numer 01AC604] Dyski do użycia jako rozszerzenie pojemności użytkowej w macierzy. | Podać part numer części:…………………………. |
| 4 | **Doposażenie posiadanej macierzy w przełącznik SAS** |  |
|  | Przełącznik SAS 12GB/s minimum 12 portowy, do montażu w szafie serwerowej RACK 19”. Porty mini SAS HD. | Podać model:…………………………. |
| 3 | **Gwarancja** |  |
|  | Gwarancja nie może być krótsza niż 12 miesięcy od daty dostawy. W przypadku zaoferowania nowej macierzy gwarancja nie może być krótsza niż 60 miesięcy. | TAK / NIE\*uzupełnić..……………… miesięcy |
|  | Czas usunięcia awarii max. 14 dni roboczych (zgodnie z zadeklarowanym terminem w formularzu ofertowym od momentu pisemnego zgłoszenia awarii, sprzęt do naprawy i z naprawy Wykonawca dostarcza na swój koszt | TAK / NIE \* |
| 4 | **Pozostałe** |  |
|  | W przypadku zaoferowania drugiej półki dyskowej elementy muszą być produktami producenta posiadanej przez Zamawiającego macierzy lub przez niego certyfikowane.W przypadku zaoferowania nowej macierzy elementy muszą być kompatybilne ze sobą.   | TAK / NIE\* |
|  | W przypadku uszkodzenia pamięci masowej (dysku/ów) uszkodzona pozostaje własnością Zamawiającego | TAK / NIE\* |

**\* niewłaściwe skreślić lub właściwe zaznaczyć**

1. W kolumnie „Faktyczne (oferowane przez Wykonawcę) parametry” w pozycjach TAK/NIE\* zaznaczanie odpowiedzi NIE oznacza niespełnienie wymaganych przez Zamawiającego parametrów.
2. Wszystkie zaoferowane elementy przedmiotu zamówienia muszą być kompatybilne z rozbudowywaną macierzą (w przypadku zaoferowania drugiej półki) lub w przypadku zaoferowania nowej macierzy kompatybilne ze sobą
* Oświadczamy, że w/w przedmiot zamówienia spełnia wszystkie wymienione w powyższej tabeli oraz w uwagach pod tabelą wymagania.

................................................................................. czytelny podpis i pieczęć osoby uprawnionej/

 osób uprawnionych do reprezentowania Wykonawcy