**OPIS PRZEDMIOTU ZAMÓWIENIA**

1. **Stacja robocza – 54 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Typ | Komputer stacjonarny. |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do Internetu oraz poczty elektronicznej |
| Wydajność | Komputer, w oferowanej konfiguracji, musi osiągać w teście wydajności SYSMARK 25 Overall Rating, wynik 1500 pkt. **Wydruk z oprogramowania testującego załączyć do oferty.**  Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS ( tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).  Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego |
| Pamięć operacyjna | 16GB DDR4 z możliwością rozbudowy do 64GB |
| Parametry pamięci masowej | 256GB SSD |
| Grafika | Osiągająca w teście PassMark 3D Grpahics Mark 1500 punktów - **załaczyć do oferty wydruk ze strony** [**https://www.videocardbenchmark.net**](https://www.videocardbenchmark.net) lub [**https://www.passmark.com**](https://www.passmark.com) |
| Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, 2 kanałowa; |
| Obudowa | Obudowa zaprojektowana i wykonana na zlecenie producenta komputera. Możliwość montażu niskoprofilowych kart graficznych, montaż beznarzędziowy dysku 3,5" oraz 2,5”, napędu optycznego i kart rozszerzeń.  Możliwość montażu dysku 2,5" oraz 3,5" wewnątrz obudowy  Zatoki na dyski i napędy: 2× 2,5/3,5, 1× 3,5, 1x 5,25;  2 porty 3.1 oraz złącza mikrofonu i słuchawek z przodu obudowy  Wbudowana karta sieciowa 10/100/1000  Możliwość otwierania bez użycia narzędzi;  Kensington Lock i ucho na kłódkę  Zasilacz o mocy 300W 80+ Bronze.  Fabrycznie zamontowane filtry przeciwkurzowe, umiejscowione na froncie, pod zasilaczem oraz na topie obudowy.  Kontroler obrotów na 6 wentylatorów |
| BIOS | * BIOS zgodny ze specyfikacją UEFI * Możliwość obsługi klawiaturą oraz myszą * Możliwość, bez uruchamiania systemu operacyjnego, odczytania z BIOS informacji o: * wersji BIOS, * nr seryjnym komputera, * ilości pamięci RAM, * typie procesora, * pojemności zainstalowanego dysku twardego * rodzajach napędów optycznych * kontrolerze audio * Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego * Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń   BIOS ma być w pełni obsługiwany przez interfejs myszy i klawiatury oraz w pełni wykorzystywać dyski twarde większe niż 2.2TB |
| Certyfikaty i standardy | Komputer musi być wyprodukowany zgodnie z normami ISO 27001 i ISO 280001 – **certyfikaty załączyć do oferty;** |
| Oprogramowanie użytkowe | Oprogramowanie umożliwiające zdalną i lokalną administrację oferowanych komputerów oraz ich diagnostykę, pozwalające na:   * zdalną i lokalną inwentaryzację komponentów komputera * zdalne i lokalne monitorowanie stanu komponentów: CPU, pamięci RAM, HDD, wersje BIOS * zdalne włączenie, wyłączanie oraz restart komputera w sieci, * monitorowanie i alertowanie zajętości dysków twardych wraz z przedstawieniem wartości w postaci wykresów. * otrzymywanie informacji WMI – Windows Management Interface * interfejs komunikacyjny w języku polskim.   W celu zapewnienia pełnej kompatybilności oprogramowania z komputerem, musi być ono wyprodukowane w całości przez producenta komputera. |
| Wbudowane porty | Wbudowane porty:   * 1 x DVI lub VGA, * 1 x HDMI ver. 1.4 * 6 portów USB wyprowadzonych na zewnątrz komputera w tym 2 porty USB 3.2 z przodu obudowy, 4szt. USB 3.2 z tyłu obudowy.   Wymagana ilość i rozmieszczenie portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, kart PCIe itp.  Porty słuchawek i mikrofonu na przednim oraz tylnym panelu obudowy.  Komputer musi umożliwiać rozbudowę w postaci dedykowanych kart PCIe;  Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL; PXE 2.1.  Płyta główna zbudowana w oparciu o kondensatory polimerowe o podwyższonej trwałości, wyposażona w:   * SATA III (6 Gb/s) - 4 szt. * M.2 - 2szt. * PCIe 3.0 x16 - 1 szt. * PCIe 3.0 x1 - 2szt. * 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM DDR4-3200 MHz;   Klawiatura USB w układzie polski programisty  Mysz USB z klawiszami oraz rolką (scroll)   * Wsparcie dla konfiguracji RAID   Wbudowany w płytę główną układ przetwarzania energii, zapewniający możliwość całościowego zarządzania poziomem zużywanej energii poprzez wykrywanie aktualnego poziomu wykorzystania zasobów PC (CPU, GPU, HDD, zasilacza) oraz inteligentne przydzielanie mocy w czasie rzeczywistym. Układ działający automatycznie od momentu uruchomienia komputera.  Ochrona przed nadmiernym napięciem zasilania:  System zasilania chroniący obwód, zaprojektowany przez producenta płyty głównej, z wbudowanymi regulatorami napięcia do ochrony chipsetu, gniazd połączeniowych i kodeków audio przed uszkodzeniem spowodowanym nieoczekiwanymi napięciami wysokiej wartości z niestabilnych albo wadliwych zasilaczy. |
| Wsparcie techniczne | Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu darmowego oprogramowania producenta lub bezpośrednio z sieci Internet po podaniu numeru seryjnego lub modelu komputera |
| Warunki gwarancji i serwisu | 3-letnia gwarancja producenta;  Czas reakcji serwisu, do końca następnego dnia roboczego.  Oferent musi posiadać ISO 9001 i ISO27001 na serwis rozwiązań informatycznych – **certyfikat załączyć do oferty** |
| System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: 2. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 3. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 4. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 5. Interfejs użytkownika dostępny w języku polskim i angielskim 6. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 7. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 8. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego; 9. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 10. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 11. Graficzne środowisko instalacji i konfiguracji w języku polskim 12. Wbudowany system pomocy w języku polskim. 13. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 14. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. 15. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 16. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 17. Zabezpieczony hasłem hierarchiczny dostęp do systemu; 18. Konta i profile użytkowników zarządzane zdalnie; 19. Praca systemu w trybie ochrony kont użytkowników. 20. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; 21. Możliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 22. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika 23. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 24. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 25. Oprogramowanie dla tworzenia kopii zapasowych (Backup); 26. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 27. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 28. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 29. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu); 30. Wbudowany mechanizm wirtualizacji typu hypervisor; 31. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. 32. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego. 33. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; 34. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 35. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; 36. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików; 37. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. 38. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. 39. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; 40. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 41. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; 42. Możliwość tworzenia wirtualnych kart inteligentnych. 43. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 44. Wsparcie dla IPSEC oparte na politykach; 45. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 46. Mechanizmy logowania w oparciu o: 47. Login i hasło, 48. Karty inteligentne i certyfikaty (smartcard), 49. Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM; 50. Umożliwiający pracę w domenie; 51. Parycja recovery umożliwiająca w przypadku awarii dysku twardego ponowną instalację zainstalowanego systemu operacyjnego oraz nośnik zawierający sterowniki wszystkich zainstalowanych urządzeń |

1. **Laptop – 2 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej |
| Ekran | Matryca IPS, 17,3” z podświetleniem w technologii LED, rozdzielczość: FHD 1920x1080, 220nits |
| Obudowa | Obudowa komputera matowa, zawiasy metalowe.  Kąt otwarcia matrycy 140 stopni.  W obudowę wbudowane co najmniej 2 diody sygnalizujące stan naładowania akumulatora oraz pracę dysku twardego. |
| Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejs SATA III (6 Gb/s) do obsługi dysków twardych. |
| Wydajność | Komputer, w oferowanej konfiguracji, musi osiągać w teście wydajności BAPCO Sysmark 25 Overall Rating wynik 1200 pkt. **Wydruk z oprogramowania testującego załączyć do oferty.**  Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS ( tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).  Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego |
| Pamięć RAM | 16 GB z możliwością rozbudowy do 32 GB RAM. DDR4 |
| Pamięć masowa | 512GB SSD 2.5 lub M2 zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |
| Grafika | Komputer, w oferowanej konfiguracji, musi osiągać w teście Sysmark25 Creativity 1300 pkt.  **Wydruk z oprogramowania testującego załączyć do oferty.** |
| Audio/Video | Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo 2 x 2W, wbudowany mikrofon, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute), kamera HD720p |
| Porty/złącza | 3 x USB 3.2 w tym 1x USB typ-C, złącze słuchawek i złącze mikrofonu typu COMBO, 1 x HDMI, 1 x RJ45 (1GBs) |
| Klawiatura | Klawiatura numeryczna, układ US z wbudowanym podświetleniem. |
| WiFi | Wbudowana karta sieciowa, pracująca w standardzie AC |
| Bluetooth | Wbudowany moduł Bluetooth 5.0 |
| Bateria i zasilanie | Czas pracy na baterii komputera w oferowanej konfiguracji - 7 godzin, potwierdzony wynikiem testu MobileMark25 Battery Life - **do oferty załączyć wynik testu testu lub link do publikacji na stronie BAPCO, w oferowanej konfiguracji**;  Zasilacz o mocy 65W; |
| BIOS | BIOS zgodny ze specyfikacją UEFI. Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego, następujących informacji: - wersji BIOS  - nr seryjnym komputera  - ilości pamięci RAM  - typie procesora i jego prędkości  -modele zainstalowanych dysków twardych  Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:   * - ustawienia hasła dla twardego dysku * - ustawienia hasła na starcie komputera tzw. POWER-On Password * - ustawienia hasła Administratora i użytkownika BIOS * - włączania/wyłączania wirutalizacji z poziomu BIOSU * - Wyłączania/Włączania: zintegrowanej karty WIFI, portów USB, trybu PXE dla karty sieciowej,   Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. |
| Waga i wymiary | Maksymalnie 2,5 kg. z baterią |
| Certyfikaty | Komputer musi być wyprodukowany zgodnie z normami ISO 9001 i ISO 50001 – **certyfikaty załączyć do oferty;** |
| Bezpieczeństwo | TPM 2.0;  Złącze Kensington Lock; |
| Warunki gwarancyjne | Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej.  Możliwość weryfikacji statusu naprawy urządzenia po podaniu numeru seryjnego  3-letnia gwarancja, czas reakcji serwisu, do końca następnego dnia roboczego. Oferent musi posiadać ISO 9001 i ISO27001 na serwis rozwiązań informatycznych – **certyfikat załączyć do oferty** |
| System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: 2. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 3. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 4. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 5. Interfejs użytkownika dostępny w języku polskim i angielskim 6. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 7. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 8. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego; 9. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 10. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 11. Graficzne środowisko instalacji i konfiguracji w języku polskim 12. Wbudowany system pomocy w języku polskim. 13. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 14. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. 15. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 16. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 17. Zabezpieczony hasłem hierarchiczny dostęp do systemu; 18. Konta i profile użytkowników zarządzane zdalnie; 19. Praca systemu w trybie ochrony kont użytkowników. 20. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; 21. Możliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 22. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika 23. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 24. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 25. Oprogramowanie dla tworzenia kopii zapasowych (Backup); 26. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 27. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 28. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 29. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu); 30. Wbudowany mechanizm wirtualizacji typu hypervisor; 31. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. 32. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego. 33. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; 34. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 35. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; 36. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików; 37. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. 38. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. 39. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; 40. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 41. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; 42. Możliwość tworzenia wirtualnych kart inteligentnych. 43. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 44. Wsparcie dla IPSEC oparte na politykach; 45. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 46. Mechanizmy logowania w oparciu o: 47. Login i hasło, 48. Karty inteligentne i certyfikaty (smartcard), 49. Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM; 50. Umożliwiający pracę w domenie; |

1. **Monitor – 10 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Przekątna ekranu | 23,8 cala; |
| Podświetlenie | LED |
| Format obrazu | 16:9 |
| Rozdzielczość | 1920 x 1080 |
| Czas reakcji matrycy | Maksymalnie 8 ms. |
| Jasność | 250  cd/m2; |
| Katy widzenia | 178 stopni pion/poziom; |
| Tilt | -5 do 20 stopni; |
| Głośniki | 2 x 2W; |
| Porty | 1 x VGA, 2 x HDMI; |
| Pobór prądu podczas pracy | Maksymalnie 25W; |
| Wymagania dodatkowe | Kompatybilność ze standardem VESA; |
| Gwarancja | 3 lata; |

**Zasilacz awaryjny – 65 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Moc znamionowa/ konfigurowalna | 320/350 VA |
| Typ obudowy | tower |
| Prąd wejściowy | Maksymalnie 10A; |
| Rodzaj wejścia | IEC C14; |
| Wyjście | 3 x IEC C13; |
| Czas przełączania zasilania | Maksymalnie 10 ms. |
| Spełniane normy | EN 50091-1, EN 50091-2; |
| Rozpraszanie ciepła | Maksymalnie 20 Btu/h; |
| Efektywność przy pełnym obciążeniu | 98% |
| Napięcie akumulatora | Maksymalnie 12V; |
| Pojemność akumulatora | 7 Ah; |
| Znamionowa energia przepięcia | 300J; |
| Czas pełnego ładowania baterii | Maksymalnie 6h; |
| Panel przedni | Wyświetlacz statusu led ze wskaźnikiem pracy online;  Zasilanie akumulatorowe;  Wskaźniki wymień baterię i przeciążenie; |
| Alarm dźwiękowy | Przy bardzo niskim poziomie naładowania akumulatora oraz sygnalizujący przeciążenie; |
| Warunki gwarancji | 2 lata; |

1. **Serwer NAS – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Procesor | Musi osiągać wynik 1900 w teście PassMark CPU Mark – **załączyć do oferty wydruk ze strony** [**www.cpunechmark.net**](http://www.cpunechmark.net) **lub** [**www.passmark.com**](http://www.passmark.com) |
| Pamięć systemowa | 2 GB z możliwością rozbudowy do 6GB; |
| Kieszenie na dyski | 2 szt.; |
| Obsługiwane dyski | 2,5 cala SSD SATA oraz 2,5 cala oraz 3,5 cala SATA ; hot swap; |
| Porty | 2 z GbE z obsługą link aggregation i/lub przełączania awaryjnego;  2 x USB 3.2; |
| Obudowa | Tower lub rack |
| Rzoozpraszanie ciepła podczas pracy | 50 BTU/hr; |
| Zasilacz | Maksymalnie 60W; |
| Wentylator | 1 x 90 mm; |
| Zainstalowane dyski | 2 x 8 TB SATA 6 Gb/s;  Czujnik drgań ruchu obrotowego;  WRL – 180;  Sterowanie odzyskiwaniem danych po wystąpieniu błędu;  MTBF – 1 mln. godzin,  Prędkość obrotowa – 7200 rpm;  Szybkość transmisji danych – 210 MB/s.;  Pamięć podręczna – 256 MB;  Odporność na wstrząsy podczas pracy – 70G;  Gwarancja – 3 lata;  Głośność podczas pracy – maksymalnie 35 dBA;  Pobór mocy podczas pracy – maksymalnie 15 W; |
| Pobór mocy podczas pracy | Maksymalnie 15W; |
| System operacyjny | 1. Obsługiwany rozmiar woluminu – 100 TB; 2. Liczba wolumenów wewnętrznych – 64; 3. SSD TRIM; 4. Powiększenie wolumenu za pomocą większych dysków twardych; 5. Powiększenie wolumenu przez dodanie dysków twardych; 6. Obsługa protokołów plików - SMB/AFP/NFS/FTP; 7. Integracja listy kontroli dostępu (ACL); 8. Uwierzytelnienie NFS Kerberos: 9. Liczba lokalnych kont użytkowników – 2048; 10. Liczba lokalnych grup – 256;; 11. Liczba folderów udostępnionych – 256; 12. High Availability; 13. Obsługiwane protokoły sieciowe - CIFS, SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP; 14. Obsługa RAID - JBOD, RAID 0, 1; 15. Migracja RAID; 16. Obsługa zbiorczego tworzenia użytkowników; 17. Obsługa dodawania użytkowników do więcej niż jednej grupy użytkowników; 18. Obsługa konfiguracji siły hasła i reguł wygaśnięci 19. Możliwość samodzielnego resetowania hasła w przypadku użytkowników niebędących administratorami; 20. Możliwość dostosowania ustawień uprawnień dla poszczególnych folderów i plików dla użytkowników i grup 21. Możliwość dostosowania ustawień uprawnień aplikacji dla użytkowników, grup i adresów IP; 22. Obsługa limitów konfiguracji wolumenów/folderów współdzielonych w celu kontrolowania maksymalnej ilości miejsca dostępnego dla każdego użytkownika; 23. Obsługa limitów szybkości dla użytkowników i grup dla protokołów FTP; 24. Liczba użytkowników lokalnych - 16 000 25. Liczba grup lokalnych – 512 26. Dostosowywanie okresu ważności hasła; 27. Wszyscy użytkownicy domyślnie muszą należeć do jednej grupy; 28. Konto „admin” musi mieć pełne uprawnienia dostępu do wszystkich usług i aplikacji na serwerze NAS; 29. Administrator musi mieć nieograniczony limit dla wolumenów i folderów współdzielonych; 30. Obsługa ustawień uprawnień dostępu użytkowników domeny/LDAP i grup do folderów współdzielonych i aplikacji; 31. Obsługa ustawień limitu dla użytkowników i grup domeny/LDAP 32. Obsługa ograniczeń szybkości transferu usług używanych przez użytkowników i grupy domeny/LDAP 33. Obsługa folderów domowych dla użytkowników domeny/LDAP 34. Obsługa zaufanych domen; 35. Możliwość przyłączania do domeny z kontrolerem domeny; 36. Możliwość przypisywania do lokalnych grup administratorów; 37. Możliwość określania przez administratora adresu IP kontrolera domeny; 38. Obsługa grup zagnieżdżonych oraz przesunięć UID/GID 39. Obsługa zintegrowanego uwierzytelniania systemu Windows; 40. Obsługa serwera SSO; |
| Gwarancja | 2 lata; |
| Wymagania dodatkowe | Kontrolki LED z regulacją jasności, przywracanie zasilania, możliwość zaplanowania włączania/wyłączania, funkcja Wake on LAN / WAN, |

1. **Urządzenie wielofunkcyjne A3 – 2 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Typ urządzenia | Laser lub LED, kolor |
| Panel LCD | 10 cali; |
| Prędkość kopiowania A4 mono i kolor | 25 str. A4 minutę |
| Czas wydruku pierwszej kopii kolor | Maksymalnie 10 sekund |
| Czas przygotowania do pracy | Maksymalnie 25 sekund |
| Formaty kopii | A3 – A6 |
| Pojemność kaset na papier A3 i A4 | 2 x 500 arkuszy |
| Pojemność podajnika ręcznego | 100 arkuszy; |
| Podajnik automatyczny | 100 arkuszy; |
| Pojemność tacy wyjścia | 250 arkuszy; |
| Funkcje drukarki | Drukowanie sieciowe, PCL 5c; PostScript 3; XPS |
| Funkcea skanera | Kolorowe skanowanie sieciowe z szybkością 80 stron mono i kolor na minutę, skan do e-mail, FTP, USB, zapis na dysku wewnętrznym;  Format wyjściowy skanów: JPEG, TIFF, PDF, Compact PDF, PDF z hasłem, XPS, Compact XPS; |
| Porty komunikacyjne | * 1 GbE, USB 2.0; |
| Pamięć | * 4 GB + wbudowany sysk SSD o pojemności 250 GB: |
| Zabezpieczeni danych na dysku wewnętrznym | - Szyfrowane hasło do dysku twardego;  - Hasło administratora;   * - Hasło administratora do skrzynki; |
| Materiały eksploatacyjne dostarczone z urządzeniem | Oryginalne tonery producenta urządzenia CMYK na 28 000 stron A4;  Bęben/y czarny na 150 000 stron A4 oraz CMY na 60 000 stron A4 każdy;  Urządzenia muszą posiadać oryginalne, fabrycznie nowe, nie regenerowane materiały eksploatacyjne (bębny i tonery) producenta urządzeń |
| Certyfikaty | Serwis musi być świadczony zgodnie z normami ISO 9001 oraz ISO 27 0001 przez producenta urządzenia lub autoryzowanego partnera serwisowego – **załączyć do oferty certyfikaty i potwierdzenie autoryzacji przez producenta urządzenia jeśli dotyczy;** |
| OCR | Dostępna z panelu urządzenia funkcja sieciowego OCR o następujących funkcjonalnościach:   1. OCR musi być zintegrowane z wyposażonymi w panel dotykowy urządzeniami; 2. OCR nie może obciążać swoim działaniem komputerów użytkowników i nie może wymagać instalacji dodatkowego oprogramowania; 3. OCR musi umożliwiać pozyskiwanie treści z dokumentów papierowych lub elektronicznych umieszczonych w katalogu sieciowym, a następnie przetwarzać je do elektronicznego pliku w formacie edytowalnym, w tym co najmniej: doc, docx, xls, xlsx lub pdf, pdf/a (z możliwością wyszukiwania tekstu) w języku polskim; 4. OCR musi umożliwiać rozpoznawanie pól i kodów kreskowych; 5. OCR musi umożliwiać rozdzielanie dokumentów za pomocą przekładek w postaci pustych stron; 6. OCR musi umożliwiać rozdzielanie dokumentów za pomocą kodów kreskowych; 7. OCR musi umożliwiać tworzenie plików XLS z zachowywaniem tła komórek, konwersji tekstu na liczby, zachowywanie kolorów tekstu, usuwanie formatowania tekstu, rozpoznawanie tylko tabel; 8. OCR musi umożliwiać tworzenie przeszukiwalnych plików PDF z opcjami, jako tekst nad obrazie, obraz na tekście, tekst i obraz, tylko obraz; 9. OCR musi umożliwiać przesłanie pozyskanej treści dokumentu w postaci pliku, poprzez wiadomość elektroniczną na skrzynkę pocztową użytkownika, bezpośrednio po zakończeniu OCR dokumentu. 10. System musi umożliwiać zdefiniowanie maksymalnego rozmiaru skanowanego pliku wysyłanego pocztą e-mail, po przekroczeniu którego dokument zapisywany będzie na lokalnym zasobie sieciowym, a właściciel musi otrzymać wiadomość e-mail zawierającą link w postaci ścieżki URL, z zaszyfrowaną nazwą pliku uniemożliwiającą podejrzenie bezpośredniej lokalizacji pliku. Po jego kliknięciu użytkownik musi otrzymać możliwość otworzenia lub zapisania pliku na dysku lokalnym 11. OCR musi posiadać licencje na min 5000 skanów miesięcznie 12. OCR nie może posiadać limitu na ilość podłączonych użytkowników; |
| Funkcja zgłaszania usterek | 1. Urządzenie musi umożliwiać na wysłanie bezpośrednio z panelu urządzenia informacji o niepoprawnym działaniu, problemach z jakością wydruków/kopii, oraz innych, które nie mogą być raportowane automatycznie poprzez SNMP;. 2. Rodzaj problemu musi być dostępny do wyboru przez użytkownika w postaci gotowej listy potencjalnych usterek; 3. W przypadku usterki polegającej na złej jakości kopii/wydruku urządzenie musi pozwalać na załączenie do wysyłanej informacji skanu dokumentu, co do którego są zastrzeżenia jakościowe. 4. Wygenerowany w ten sposób alert musi zawierać dodatkowe informacje uzupełnione automatycznie przez urządzenie w postaci: numeru seryjnego urządzenia, daty, godziny; |
| Wymagania dodatkowe | Dupleks i ADF;  Oryginalna podstawa producenta urządzenia na kółkach z szafką;  Kabel zasilający 1.8m;  Kabel drukarkowy USB 1.8m;  Kabel Ethernet 3m; |
| Warunki gwarancji | 3 lata;  Cena musi uwzględniać wszystkie przeglądy niezbędne do utrzymania gwarancji;  Wykonawca zobowiązany jest w okresie gwarancji do przeprowadzenia co najmniej jednego przeglądu rocznie, obejmującego:  - Demontaż i montażu maszyny;  - Czyszczenie podzespołów: optyki, poboru i transportu papieru, i wyposażenia opcjonalnego (podajniki dokumentów, separatory itp.)  - Aktualizację oprogramowania sprzętowego  - Ocenę stanu technicznego urządzenia |

1. **Kamera internetowa – 10 szt.**

Rozdzielczość - 720 p.

Liczba klatek na sekundę – 30

Pole widzenia po przekątnej – 60 stopni;

Automatyczna korekcja natężenia światła

Niwelujący szumy mikrofon

Połączenie – USB, plu and play;

Długość kabla – 2 metry;

Gwarancja – 2 lata;

1. **Urządzenie wielofunkcyjne A4 – 15 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Typ urządzenia | Laser, mono; |
| Panel LCD | 6 cali; |
| Prędkość druku A4 /kopiowania jedno/dwustronnego | 35/30 str. na minutę |
| Czas wydruku pierwszej strony | Maksymalnie 10 sekund |
| Rozdzielczość druku /kopii | 1200 x 1200 dpi. 600 x 600 dpi; |
| Wymagane funkcje kopiowania | Sortowanie, zmniejszanie/powiększanie od 25 do 400%, ustawienia wstępne, margines na oprawę, i dwie strony na jedną stronę, dopasowanie do strony, optymalizacja pod kątem zawartości, podgląd kopii; |
| Skanowanie | ADF, dwustronne, skanowanie do chmury, do wiadomości e-mail z wyszukiwaniem adresu e-mail LDAP, do folderu sieciowego, do USB, do komputera; |
| Formaty plików skanowania | PDF, skompresowany PDF, JPEG, TIFF, , XPS, PDF/A, przeszukiwalny PDF, RTF, TXT, BMP, PNG, TIFF; |
| Procesor | 1,2 GHz; |
| Pamięć RAM | 512 MB RAM i 512 MB flash; |
| Obciążalność miesięczna dopuszczalna przez producenta | 80 000 stron |
| Obsługiwane nośniki | A4, A5, A6, B5, B6, 16K, DL, C5; |
| Pojemność tacy wejściowej | 350 arkuszy; |
| Pojemność tacy wyjściowej | 150 arkuszy; |
| Języki drukowania | PCL 6, PCL 5c,Postscript 3, PDF, URF; |
| Obsługiwane protokoły sieciowe | TCP/IP, IPv4, IPv6, LPD, SNMPv1, SNMPv2, SNMPv3, HTTP/HTTPS, Syslog, FTP FW Download; |
| Porty komunikacyjne | * 1 x 1 GbE, 2 x USB; |
| Bezpieczeństwo | * Bezpieczne uruchamianie i przeglądanie przez SSL/TLS 1.0, TLS 1.1, TLS 1.2; IPP przez TLS; * Włączanie/wyłączanie portów i funkcji sieciowych; * Wyłączanie usług, SNMPv1, SNMPv2 i SNMPv3; * HTTPS z weryfikacją certyfikatu; * HTTP Basic Access Authentication, SASL; * Uwierzytelnianie i autoryzacja LDAP; * Zapora i ACL; * Konfiguracja certyfikatów; * Drukowanie PIN UPD * Syslog; * Kontrola dostępu, uwierzytelnianie 802.1x; * Szyfrowane przechowywanie danych; * Bezpieczne usuwanie danych; * Automatyczne aktualizacje oprogramowania; |
| Wymagania dodatkowe | Automatyczny duplex; |
| Gwarancja | 12 miesięcy; |

1. **Specjalistyczne oprogramowanie – 82 szt.**

Zamawiający posiada obecnie 41 licencji oprogramowania ESET Endpoint Security z aktywną subskrypcją do dnia 13.05.2023.

Przedmiotem zamówienia jest przedłużenie obecnej subskrypcji o 3 lata tj. do dnia 13.05.2026 roku oraz rozbudowa do łącznie 82 licencji, z czego 2 licencje będą używane przez Ośrodek Pomocy Społecznej w Wołczynie

1. **Oprogramowanie biurowe – 47 szt.**

Kompletny pakiet oprogramowania biurowego musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Wymagania odnośnie interfejsu użytkownika:

1. Pełna polska wersja językowa interfejsu użytkownika;
2. Prostota i intuicyjność obsługi, pozwalająca na prace osobom

nieposiadającym umiejętności technicznych;

1. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej musi być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się;
2. Oprogramowanie musi umożliwiać tworzenie i edycje dokumentów elektronicznych w formacie, który spełnia następujące warunki:
3. posiada kompletny i publicznie dostępny opis formatu,
4. ma zdefiniowany układ informacji w postaci XML zgodnie z Tabela B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
5. umożliwia wykorzystanie schematów XML
6. wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabela A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
7. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb użytkownika oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców;
8. W skład oprogramowania muszą wchodzić narzędzia umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami;
9. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim;.
10. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
11. Edytor tekstów
12. Arkusz kalkulacyjny
13. Narzędzie do przygotowywania i prowadzenia prezentacji/ tworzenia, edytowania i wyświetlania prezentacji
14. Narzędzie do zarzadzania informacja prywatną (poczta elektroniczna, kalendarzem, kontaktami i zadaniami)
15. Edytor tekstu musi umożliwiać:
16. Edycję i formatowanie tekstu w języku polskim wraz z obsługa języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
17. Wstawianie oraz formatowanie tabel
18. Wstawianie oraz formatowanie obiektów graficznych
19. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)
20. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
21. Automatyczne tworzenie spisów treści
22. Formatowanie nagłówków i stopek stron
23. Sprawdzanie pisowni w języku polskim
24. Śledzenie zmian wprowadzonych przez użytkowników
25. Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności
26. Określenie układu strony (pionowa/pozioma)
27. Wydruk dokumentów
28. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarzadzania informacją prywatną
29. Prace na posiadanych przez zamawiającego dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu
30. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
31. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostepniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.
32. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
33. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostepniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.
34. Arkusz kalkulacyjny musi umożliwiać:
35. Tworzenie raportów tabelarycznych
36. Tworzenie wykresów liniowych (wraz linia trendu), słupkowych, kołowych
37. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
38. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
39. Obsługę kostek OLAP oraz tworzenie i edycje kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiazywanie problemów optymalizacyjnych
40. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczna zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
41. Wyszukiwanie i zamianę danych
42. Wykonywanie analiz danych przy użyciu formatowania warunkowego
43. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
44. Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności
45. Formatowanie czasu, daty i wartości finansowych z polskim formatem
46. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
47. Zachowanie pełnej zgodności z formatami posiadanych przez zamawiającego plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013 i 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń..
48. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
49. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać przygotowywanie prezentacji multimedialnych oraz:
50. Prezentowanie przy użyciu projektora multimedialnego
51. Drukowanie w formacie umożliwiającym robienie notatek
52. Zapisanie w postaci tylko do odczytu.
53. Nagrywanie narracji dołączanej do prezentacji
54. Opatrywanie slajdów notatkami dla prezentera
55. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
56. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
57. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
58. Tworzenie animacji obiektów i całych slajdów
59. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
60. Pełna zgodność z formatami plików posiadanych przez zamawiającego, utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016.
61. Narzędzie do zarzadzania informacja prywatna (poczta elektroniczna, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
62. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego
63. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców
64. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną
65. Automatyczne grupowanie poczty o tym samym tytule
66. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczna do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy
67. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia
68. Zarzadzanie kalendarzem
69. Udostępnianie kalendarza innym użytkownikom
70. Przeglądanie kalendarza innych użytkowników
71. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach
72. Zarzadzanie lista zadań
73. Zlecanie zadań innym użytkownikom
74. Zarzadzanie listą kontaktów
75. Udostępnianie listy kontaktów innym użytkownikom
76. Przeglądanie listy kontaktów innych użytkowników
77. Możliwość przesyłania kontaktów innym użytkowników
78. Licencja niewygasająca do użytku komercyjnego. Nie dopuszcza się licencji w modelu subskrypcyjnym;
79. **UTM – 1 szt.**
80. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia.
81. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
82. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
83. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie routingu, firewall’a, IPSec VPN, antywirusa, IPSa, kontroli aplikacji.
84. Musi istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.
85. System musi wspierać IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, kontrola aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach musi istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System realizujący funkcję firewall musi dysponować minimum 8 portami Gigabit Ethernet RJ-45 oraz 2 portami SFP Gigabit Ethernet.
5. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
6. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
7. System musi być wyposażony w zasilanie AC.
8. W zakresie Firewall’a obsługa nie mniej niż 1,5mln jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.
9. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
10. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.8 Gbps.
11. Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps.
12. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
13. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps
14. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTPS – minimum 700 Mbps
15. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
16. Kontrola Aplikacji.
17. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
18. Ochrona przed malware co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
19. Ochrona przed atakami - Intrusion Prevention System.
20. Kontrola stron WWW.
21. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
22. Zarządzanie pasmem (QoS, Traffic shaping).
23. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
24. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych.
25. Analiza ruchu szyfrowanego protokołem SSL.
26. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
27. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa, w tym co najmniej: DMZ, LAN, WAN.
2. Element systemu realizujący funkcję Firewall musi integrować się z rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu;
3. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

* Wsparcie dla IKE v1 oraz v2.
* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19 i 20.
* Wsparcie dla pracy w topologii Hub and Spoke oraz Mesh;
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu oraz routingu statycznego.
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

* Pracę w trybie, w którym dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

1. W zakresie routingu rozwiązanie musi zapewniać obsługę:

* Routingu statycznego.
* Policy Based Routingu.
* Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
4. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach;
5. System musi umożliwiać skanowanie archiwów, w tym co najmniej zip i RAR.
6. System musi dysponować sygnaturami do ochrony urządzeń mobilnych co najmniej dla systemu operacyjnego Android
7. System musi współpracować z platformą typu Sandbox lub usługą typu Sandbox;
8. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
9. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
10. Ochrona IPS musi opierać się na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
11. System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach.
12. Baza sygnatur ataków musi zawierać 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
13. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
14. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego;.
15. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, cookies.
16. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
17. Funkcja kontroli aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
18. Baza kontroli aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
19. Aplikacje chmurowe muszą być kontrolowane pod względem wykonywanych czynności, w tym co najmniej pobierania i wysyłania plików.
20. Baza musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
21. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
22. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
23. W ramach filtra www muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, w tym co najmniej: malware, phishing, spam, Dynamic DNS, proxy.
24. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
25. Funkcja przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek;
26. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
27. Możliwość określenia, dla których kategorii URL lub wskazanych URL system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
28. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych w oparciu o zewnętrzne bazy danych.

1. Możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie mechanizmów RADIUS lub API.
3. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i muszą mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
4. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
5. Możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
6. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
7. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
8. Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podgląd pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
9. Firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
10. Elementy systemu bezpieczeństwa muszą umożliwiać logowanie do aplikacji) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
11. Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu.
12. Możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
13. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
14. Możliwość logowania do serwera SYSLOG.
15. Certyfikat ICSA lub EAL4 dla funkcji Firewall
16. W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów.
17. Muszą one obejmować: kontrola aplikacji, IPS, antywirus analiza sandbox, antyspam, web Ffltering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.
18. System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
19. W stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), oferent winien przedłożyć dokument pochodzący od producenta lub importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) **– załączyć do oferty;**
20. Dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania – **załączyć do oferty**
21. Oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań – **załączyć do oferty.**

**Zamawiający oprócz dokumentów wymienionych powyżej, żąda załączenia do oferty kart katalogowych proponowanych sprzętów i systemów informatycznych.**

**Zamawiający zastrzega sobie możliwość wezwania oferentów, którzy złożyli oferty niepodlegające odrzuceniu w niniejszym postępowaniu, do okazania zaoferowanego sprzętu i oprogramowania, w celu sprawdzenia ich zgodności z wymaganiami określonymi przez Zamawiającego w SWZ.**

**Okazanie nastąpi w dniu wyznaczonym przez Zamawiającego, po terminie składania ofert. Zamawiający poinformuje o terminie przeprowadzenia okazania z co najmniej pięciodniowym wyprzedzeniem (dni kalendarzowe).**

**Niestawienie się oferenta w wyznaczonym czasie i miejscu na okazaniu (prezentacji) sprzętu i/lub oprogramowania, uznane będzie jako negatywny wynik okazania, tj. niepotwierdzenie przez oferenta wymagań określonych przez Zamawiającego, co będzie skutkowało odrzuceniem oferty na podstawie art. 226 ust. 1 pkt. 5 Ustawy Pzp.**