Opis przedmiotu zamówienia

* 1. Oferowane produkty muszą spełniać wszystkie parametry określone w niniejszym załączniku oraz oznakowane symbolem CE, pochodzić z legalnego źródła.
  2. Wszystkie opisane parametry wymagane są wymaganiami podstawowymi. Zamawiający akceptuje rozwiązania o parametrach równoważnych lub lepszych, bez utraty funkcjonalności i wydajności.
  3. Wszystkie oferowane produkty muszą być sprawne, fabrycznie nowe, nieużywane.

**Część 1**

**a) Komputer – 42 szt.**

|  |  |
| --- | --- |
|  | **Opis wymaganych parametrów technicznych** |
| **1** | **2** |
| 1.1 | Typ: stacjonarny All in One |
| 1.2 | Procesor: wielordzeniowy klasy x86, min. 2,10 GHz, osiągający według testu PassMark Average CPU Mark wynik min. 9900 punktów.  *Zamawiający wezwie Wykonawcę, którego oferta zostanie najwyżej oceniona  do złożenia wydruku ze strony http://www.cpubenchmark.net potwierdzającego spełnianie wymagań dla zaoferowanego urządzenia, z datą nie później niż na dzień składania ofert.* |
| 1.3 | Pamięć: 1 x min. 8GB 2666 MHz, możliwość rozbudowy do min 32GB, minimum jeden slot wolny na dalszą rozbudowę |
| 1.4 | Dysk twardy SSD min. 256 GB |
| 1.5 | Płyta główna: zgodna z technologią oferowanego modelu procesora  - 2 złącza SODIMM z obsługą do 32GB pamięci RAM 2666MHz  - sloty: 1 szt M.2 PCIe x1 dla WLAN  - 1 złącze m.2 dla dysku  - 1 złącze SATA dla dysku |
| 1.6 | Karta graficzna: zgodna z oferowanym modelem procesora |
| 1.7 | Zintegrowana karta dźwiękowa |
|  | Komunikacja:  Karta sieciowa przewodowa: 10/100/1000  Łączność bezprzewodowa: WiFi 802.11 a/b/g/n  Bluetooth |
| 1.8 | Interfejsy:   * min. 1 szt DisplayPort 1.2, * min. 1 szt HDMI * min. 5 x USB w tym min. 1 szt USB 2.0 typ-C, 4 szt USB 3.1 * port sieciowy RJ-45, * port audio COMBO * czytnik kart SD 3-in-1 * kamera internetowa 1 Mpix z dwoma mikrofonami zintegrowana w obudowie matrycy   Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, adapterów itp. |
| 1.9 | Napęd wbudowany: DVD-RW |
| 1.10 | Monitor:  rodzaj: LED  rozdzielczość [dpi]: 1920 x 1080  przekątna ekranu [cal]: 23.8  wbudowane głośniki |
| 1.11 | Zasilacz: aktywny stabilizator PFC, moc 120W |
| 1.12 | Obudowa typu All in One – zintegrowany komputer w obudowie wraz z monitorem z matrycą IPS min 23,8” o parametrach:  - rozdzielczośc min 1920 x 1080  - kontrast typowy min 1000:1,  - plamka max 0,275  - typowa jasność min 250 cd/m2 ,matryca matowa  - kąty widzenia pion/poziom: min 178/178 stopni  - kąty pochylenia matrycy w pionie min -5/+25 stopni (+/-1 stopień)  - możliwość regulacji wysokości ekranu w pionie +/- 10 cm  - obrotowa podstawa komputera , kąt obrotu +/- 45 stopni  Posiadająca min. 1 wewnętrzną półkę 2,5” umożliwiającą zamontowanie dysku 2,5”  Wymagany jest wbudowany fabrycznie dźwiękowo-wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, który musi sygnalizować co najmniej:  awarie procesora  uszkodzenie kontrolera Video  uszkodzenie pamięci RAM  Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) |
| 1.13 | System zabezpieczeń:   * DriveLock; * Czujnik otwarcia obudowy; * Hasło uruchamiania (w systemie BIOS); * Sterowanie uruchamianiem z nośników wymiennych / zapisem na nośnikach wymiennych; * Wyłączanie portu SATA (w systemie BIOS); * Hasło konfiguracji (w systemie BIOS); * Obsługa kłódkowego zabezpieczenia obudowy i linek zabezpieczających; * Moduł Trusted Platform Module TPM 2.0, * Włączanie/wyłączanie portu USB (przez BIOS); * Zabezpieczenia głównego rekordu rozruchowego; * Uwierzytelnianie przed rozruchem; * Włączanie/wyłączanie portu szeregowego (w systemie BIOS); |
| 1.14 | Waga: max 9,5 kg |
| 1.15 | System operacyjny: Windows 10 Pro 64 lub rozwiązanie równoważne.  Warunki równoważności: System operacyjny 64-bit, dołączony nośnik z oprogramowaniem. Za rozwiązanie równoważne uznaje się takie, które posiada wbudowane mechanizmy, bez użycia dodatkowych aplikacji (bez jakichkolwiek emulatorów, implementacji lub programów towarzyszących), zapewniające:  1. polską wersję językową,  2. możliwość instalacji i poprawnego działania oprogramowania dostępnego w ramach posiadanych przez Zamawiającego licencji Microsoft Office 2010, Microsoft Office 2013, Microsoft Office 2016) oraz możliwość pełnej integracji z systemem domenowym MS Windows,  3. możliwość instalacji i poprawnego działania aplikacji wykorzystywanych przez Zamawiającego, oraz poprawnej obsługi powszechnie używanych, urządzeń peryferyjnych (drukarek, skanerów, kser), 4. dostępność aktualizacji i poprawek do systemu u producenta systemu bezpłatnie i bez dodatkowych opłat licencyjnych z możliwością wyboru instalowanych poprawek,  5. możliwość zdalnej, automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu,  6. możliwość automatycznego zbudowania obrazu systemu wraz z aplikacjami, obraz systemu służyć ma do automatycznego upowszechniania systemu operacyjnego inicjowanego i wykonywanego w całości przez sieć komputerową,  7. możliwość wdrożenia nowego obrazu przez zdalną instalację,  8. graficzne środowisko instalacji i konfiguracji,  9. możliwość udostępniania i przejmowania pulpitu zdalnego,  10. możliwość udostępniania plików i drukarek,  11. możliwość blokowania lub dopuszczenia dowolnych urządzeń peryferyjnych za pomocą polityk sprzętowych (np. przy użyciu numerów identyfikacyjnych sprzętu),  12. zapewnienie wsparcia dla większości powszechnie używanych urządzeń (drukarek, urządzeń sieciowych, standardów USB, urządzeń Plug & Play, WiFi,  13. wyposażenie systemu w graficzny interfejs użytkownika w języku polskim,  14. zapewnienie pełnej kompatybilności z oferowanym sprzętem,  15. zintegrowanie z systemem modułu pomocy dla użytkownika w języku polskim,  16. zintegrowanie z systemem modułu wyszukiwania informacji,  17. możliwość wykonywania kopii bezpieczeństwa (całego dysku, wybranych folderów, kopii przyrostowych) wraz z możliwością automatycznego odzyskania wersji wcześniejszej,  18. zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników,  19. zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacja dostępna u producenta nieodpłatnie bez ograniczeń czasowych,  20. licencja na system operacyjny musi być nieograniczona w czasie, pozwalać na wielokrotne instalowanie systemu na oferowanym sprzęcie bez konieczności kontaktowania się przez Zamawiającego z producentem systemu lub sprzętu,  21. oprogramowanie powinno pochodzić z legalnego źródła i posiadać certyfikat autentyczności lub unikalny kod aktywacyjny nieużywany oraz nieaktywowany nigdy wcześniej na innym urządzeniu,  22. zamawiający nie dopuszcza w systemie możliwości instalacji dodatkowych narzędzi emulujących działanie systemów.  W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania |
| 1.16 | Oprogramowanie Microsoft Office 2019 Home and Business 2019 PL lub rozwiązanie równoważne.  Warunki równoważności:  Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej,  Wymagania odnośnie interfejsu użytkownika:  a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.  b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.  c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.  Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi katalogowej Active Directory.  Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.  Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:  a. posiada kompletny i publicznie dostępny opis formatu,  b. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526),  c. umożliwia kreowanie plików w formacie XML,  d. wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,  Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.  W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).  Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.  Pakiet zintegrowanych aplikacji biurowych musi zawierać:  a. Edytor tekstów  b. Arkusz kalkulacyjny  c. Narzędzie do przygotowywania i prowadzenia prezentacji  d. Narzędzie do tworzenia drukowanych materiałów informacyjnych  e. Narzędzie do tworzenia i pracy z lokalną bazą danych  f. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)  g. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.  h. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.  Edytor tekstów musi umożliwiać:  a. 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.  b. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.  c. Wstawianie oraz formatowanie tabel.  d. Wstawianie oraz formatowanie obiektów graficznych.  e. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).  f. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.  g. Automatyczne tworzenie spisów treści.  h. Formatowanie nagłówków i stopek stron.  i. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.  j. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.  k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.  l. Określenie układu strony (pionowa/pozioma).  m. Wydruk dokumentów.  n. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.  o. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.  p. Zapis i edycję plików w formacie PDF.  q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  r. Możliwość jednoczesnej pracy wielu użytkowników na jednym dokumencie z uwidacznianiem ich uprawnień i wyświetlaniem dokonywanych przez nie zmian na bieżąco,  s. Możliwość wyboru jednej z zapisanych wersji dokumentu, nad którym pracuje wiele osób.  Arkusz kalkulacyjny musi umożliwiać:  a. Tworzenie raportów tabelarycznych  b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych  c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.  d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)  e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych  f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych  g. Wyszukiwanie i zamianę danych  h. Wykonywanie analiz danych przy użyciu formatowania warunkowego  i. Tworzenie wykresów prognoz i trendów na podstawie danych historycznych z użyciem algorytmu ETS  j. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie  k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności  l. Formatowanie czasu, daty i wartości finansowych z polskim formatem  m. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.  n. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.  o. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).  p. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.  q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji  Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:  a. Przygotowywanie prezentacji multimedialnych, które będą:  b. Prezentowanie przy użyciu projektora multimedialnego  c. Drukowanie w formacie umożliwiającym robienie notatek  d. Zapisanie jako prezentacja tylko do odczytu.  e. Nagrywanie narracji i dołączanie jej do prezentacji  f. Opatrywanie slajdów notatkami dla prezentera  g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo  h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego  i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym  j. Możliwość tworzenia animacji obiektów i całych slajdów  k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu.  l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016.  Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:  a. Tworzenie i edycję drukowanych materiałów informacyjnych  b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.  c. Edycję poszczególnych stron materiałów.  d. Podział treści na kolumny.  e. Umieszczanie elementów graficznych.  f. wykorzystanie mechanizmu korespondencji seryjnej  g. Płynne przesuwanie elementów po całej stronie publikacji.  h. Eksport publikacji do formatu PDF oraz TIFF.  i. Wydruk publikacji.  j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.  Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać:  a. Tworzenie bazy danych przez zdefiniowanie:  b. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.  c. Relacji pomiędzy tabelami  d. Formularzy do wprowadzania i edycji danych  e. Raportów  f. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych  g. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów  h. Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.  Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:  a. Uwierzytelnianie wieloskładnikowe poprzez wbudowane wsparcie integrujące z usługą Active Directory,  b. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,  c. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,  d. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,  e. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,  f. Automatyczne grupowanie poczty o tym samym tytule,  g. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,  h. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,  i. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,  j. Zarządzanie kalendarzem,  k. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,  l. Przeglądanie kalendarza innych użytkowników,  m. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,  n. Zarządzanie listą zadań,  o. Zlecanie zadań innym użytkownikom,  p. Zarządzanie listą kontaktów,  q. Udostępnianie listy kontaktów innym użytkownikom,  r. Przeglądanie listy kontaktów innych użytkowników,  s. Możliwość przesyłania kontaktów innym użytkowników,  t. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.  Oprogramowanie powinno pochodzić z legalnego źródła i posiadać certyfikat autentyczności lub unikalny kod aktywacyjny nieużywany oraz nieaktywowany nigdy wcześniej na innym urządzeniu.  Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu.  Okres licencji: Bezterminowa |
| 1.17 | Dołączone wyposażenie: |
| Klawiatura: standard – USB, ciche klawisze |
| Mysz optyczna, rolka, standard – USB |
| 1.18 | Certyfikaty i standardy: |
| Certyfikat jakości ISO 9001: 2000 producenta komputera |
| Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera |
| 1.19 | Gwarancja – min.36 miesięcy |

**b) Drukarka laserowa mono – szt. 10**

|  |  |
| --- | --- |
|  | **Opis wymaganych parametrów technicznych** |
| **1** | **2** |
| 1.1 | Technologia druku – laserowa |
| 1.2 | Automatyczny druk dwustronny |
| 1.3 | Czas wydruku pierwszej strony w czerni [s] – max 6 s |
| 1.4 | Standardowa jakość druku w czerni – min. 600x600 dpi |
| 1.5 | Standardowa pojemność pamięci [MB] – 256 |
| 1.6 | Maksymalna pojemność pamięci [MB] – 256 |
| 1.7 | Szybkość procesora – 1500 MHz |
| 1.8 | Waga drukarki [kg] max. 12 kg |
| 1.9 | Głośność: Poziom mocy akustycznej: maksymalni 4,0 B(A)  Ciśnienie akustyczne: LpAm maksymalnie 54 dB(A) |
| 1.10 | Pojemność podajnika standardowego [arkusze] – min.100 |
| 1.11 | Pojemność podajnika kasety głównej [arkusze] – min.550 |
| 1.12 | Obsługiwane formaty nośników: A4, A5, A6, B5 |
| 1.13 | Panel sterowania:  wyświetlacz LCD, |
| 1.14 | Maksymalne zużycie: 780 W (aktywność), 14,5 W (oczekiwanie), 8,5 W (tryb Powersave), 0,6 W (urządzenie wyłączone) |
| 1.15 | Zgodność z systemami operacyjnymi: System operacyjny Windows z obsługą sterownika dołączonego do produktu: Wszystkie wersje systemu Windows 10 32-bitowe/64-bitowe (z wyłączeniem systemu RT OS dla tabletów), wszystkie wersje systemu Windows 8/8.1 32-bitowe/64-bitowe (z wyłączeniem systemu RT OS dla tabletów), wszystkie wersje systemu Windows 7 32-bitowe/64-bitowe, wszystkie wersje systemu Windows Vista 32-bitowe (Home Basic, Premium, Professional itp.) |
| 1.16 | Obsługiwane gramatury nośników:  od 60 do 220 g/m² |
| 1.17 | Łączność:  Szybkie porty Host/Device USB 2.0 Interfejs Fast Ethernet 10Base-T/100Base-TX, Gigabit Ethernet 1000Base-T |
| 1.18 | Języki opisu strony/emulacje:  PCL 5, PCL 6, Postscript Level 3, PDF |
| 1.19 | Kabel USB, ekranowany z ferrytem |
| 1.20 | Materiały eksploatacyjne:  Toner dostarczany jako pojedynczy kartridż |
| 1.21 | CD (zawiera oprogramowanie i podręcznik użytkownika) |
| 1.22 | Kabel zasilania |
| 1.23 | Gwarancja – minimum 12 miesiące |

* 1. **Urządzenie wielofunkcyjne kolorowe – szt. 1**

|  |  |
| --- | --- |
|  | **Opis wymaganych parametrów technicznych** |
| **1** | **2** |
| 1.1 | Obsługiwana wielozadaniowość  Funkcje: drukowanie, kopiowanie, skanowanie, faksowanie |
| 1.2 | Panel sterowania: Ekran dotykowy LCD (kolorowy, graficzny) |
| 1.3 | Waga drukarki netto [kg] max. 41 kg |
| 1.4 | Głośność: Ciśnienie akustyczne: LpAm maksymalnie 52 dB(A) |
| 1.5 | Maksymalne zużycie: 605 W (drukowanie), 440 W (kopiowanie), 52 W (tryb gotowości), 8,1 W (tryb uśpienia), 0,3 W (urządzenie wyłączone). |
| 1.6 | Zgodność z systemami operacyjnymi: Windows 10, Windows 8, Windows 7 (32/64-bitowy),: Procesor 1 GHz 32-bitowy (x86) lub 64-bitowy (x64), 1 GB pamięci RAM (32-bitowy) lub 2 GB pamięci RAM (64-bitowy), napęd CD/DVD-ROM lub połączenie z internetem, port sieciowy lub USB; |
| 1.7 | Łączność:  1 port Hi-Speed USB 2.0; 1 port USB hosta; 1 port sieciowy Gigabit Ethernet 10/100/1000T; 1 port RJ-11 (faks); 1 port RJ-11 (wyłącznie telefon) |
| 1.8 | Języki opisu strony/emulacje:  PCL 5, PCL 6, Postscript Level 3, PDF |
| 1.9 | Drukowanie:   * Automatyczny druk dwustronny * Prędkość druku czerń i kolor: do 30 str./min * Wydruk pierwszej strony w czerni, A4, po wyjściu ze stanu gotowości: max. 10,5 s * Jakość druku w czerni i kolorze – do 600x600 dpi * Standardowa pojemność pamięci [MB] – 256 * Maksymalna pojemność pamięci [MB] – 256 * Szybkość procesora – 800 MHz * Podajniki: uniwersalny na 100 arkuszy, podajnik 2 na 250 arkuszy, automatyczny podajnik dokumentów na 50 arkuszy * Obsługiwane formaty nośników: A4, A5, A6, B5 * Nośniki: Papier (typu bond, broszurowy, kolorowy, błyszczący, firmowy, fotograficzny, zwykły, wstępnie zadrukowany, dziurkowany, makulaturowy, szorstki), kartki pocztowe, folie, etykiety, koperty * Gramatura nośników: * podajnik 1: 60–216 g/m² (zwykły papier), 105–220 g/m² (papier błyszczący); * podajnik 2: 60–163 g/m² (zwykły papier), 105–220 g/m² (papier błyszczący); * automatyczny podajnik dokumentów: od 60 do 90 g/m2 |
| 2.0 | Skanowanie:   * Skaner płaski, automatyczny podajnik dokumentów * Rozdzielczość skanowania: Maks. 300 x 300 dpi (w kolorze i w czerni, automatyczny podajnik dokumentów);  Maks. 1200 x 1200 dpi (w kolorze i w czerni, szyba); * Maksymalny format skanowania (automatyczny podajnik dokumentów):  216 x 356 mm * Minimalny format skanowania (automatyczny podajnik dokumentów):  127 x 177 mm * Szybkość skanowania (tryb normalny, format A4): do 19,5 str./min w czerni, do 14 str./min w kolorze * Dwustronne skanowanie z automatycznego podajnika dokumentów, dwustronne skanowanie w kolorze * Pojemność automatycznego podajnika dokumentów: standardowo 50 arkuszy |
| 2.1 | Kopiowanie:   * Prędkość kopiowania w czerni, tryb normalny, format A4: do 30 kopii/min * Rozdzielczość kopii w czerni i kolorze: do 300 x 300 dpi |
| 2.2 | Faksowanie:  Prędkość przesyłania faksu: 33,6 kb/s  Pamięć faksu: do 250 stron  Rozdzielczość faksu w czerni: do 300 x 300 dpi |
| 2.3 | Materiały eksploatacyjne: Wkład z czarnym tonerem (~5500 stron), wkłady z tonerem błękitnym, purpurowym i żółtym (~6000 stron), |
| 2.4 | CD (zawiera oprogramowanie i podręcznik użytkownika) |
| 2.5 | Kabel zasilania |
| 2.6 | Gwarancja – minimum 12 miesięcy |

**d) Drukarka laserowa kolorowa – szt. 1**

|  |  |
| --- | --- |
|  | **Opis wymaganych parametrów technicznych** |
| **1** | **2** |
| 1.1 | Technologia druku – laserowa kolorowa |
| 1.2 | Automatyczny druk dwustronny |
| 1.3 | Parametry druku:   * rozdzielczość druku mono min. 1200x1200 dpi * rozdzielczość druku w kolorze min. 1200x1200 dpi * szybkość drukowania mono do 33 stron A4/min * szybkość drukowania w kolorze do 33 stron A4/min * czas do wydruku pierwszej strony mono do 6 sekund * czas do wydruku pierwszej strony w kolorze do 7 sekund |
| 1.4 | Obsługa Nośników   * gramatura dla podajnika standardowego do 220 g/m² * maksymalna gramatura papieru do 220 g/m² * podajnik na pojedyncze arkusze tak * ręczne podawanie nośników tak * pojemność podajnika standardowego [arkusze] – min. 100 * pojemność podajnika kasety głównej [arkusze] – min. 550 * ilość odbiorników papieru 1 * pojemność odbiornika papieru min. 250 arkuszy * niestandardowe wymiary nośników (szerokość) min 76 mm max 216 mm * niestandardowe wymiary nośników (długość) min 127 mm max 356 mm * obsługiwane rodzaje nośników: papier zwykły, papier o niskiej gramaturze, papier bond, papier makulaturowy, papier błyszczący, papier o wysokiej gramaturze, papier o wysokiej gramaturze błyszczący, karton, papier formatu pocztówkowego błyszczący, folie kolorowe, etykiety, papeteria firmowa, koperty, papier wstępnie zadrukowany, papier dziurkowany, papier kolorowy, papier szorstki, folie nieprzejrzyste * obsługiwane formaty nośników: A4, RA4, A5, B5 (JIS), B6 (JIS), A6, koperty (B5, C5 ISO, C6, DL ISO) |
| 1.5 | Standardowa pojemność pamięci [MB] – 1024 |
| 1.6 | Maksymalna pojemność pamięci [MB] – 1024 |
| 1.7 | Szybkość procesora – 1200 MHz |
| 1.8 | Pojemność dysku twardego: 4GB pamięci trwałej, szyfrowanie danych klientów/zadań |
| 1.9 | Waga drukarki netto [kg] max. 28 kg |
| 1.10 | Głośność:  Ciśnienie akustyczne: LpAm maksymalnie 51 dB(A) |
| 1.11 | Panel sterowania:  wyświetlacz LCD (kolorowy, graficzny), |
| 1.12 | Maksymalne zużycie: 571 W (drukowanie), 33,2 W (tryb gotowości), 3,90 W (tryb uśpienia), 1 W (tryb automatycznego wyłączenia), 0,1 W (urządzenie wyłączone) |
| 1.13 | Zgodność z systemami operacyjnymi: Windows 10 32-bit i 64-bit (z wyłączeniem systemu RT OS do tabletów), Windows 8/8.1 32-bit i 64-bit (z wyłączeniem systemu RT OS do tabletów)  Windows 7 32-bit i 64-bit, Windows Vista 32-bit |
| 1.14 | Łączność:  Port USB 2.0 Hi-Speed; Wbudowany port sieci Fast Ethernet 10/100/1000Base-TX |
| 1.15 | Języki opisu strony/emulacje:  PCL 5, PCL 6, Postscript 3, PDF |
| 1.16 | Materiały eksploatacyjne:  Cztery zainstalowane fabrycznie wkłady z tonerem (wydajność ~6000 stron w czerni i ~5000 stron w kolorze), Zestaw do zbierania tonera, |
| 1.17 | CD (zawiera oprogramowanie i podręcznik użytkownika) |
| 1.18 | Kabel zasilania |
| 1.19 | Gwarancja – minimum 12 miesiące |

**e) UPS – 1 szt.**

|  |  |
| --- | --- |
|  | **Opis wymaganych parametrów technicznych** |
| **1** | **2** |
| 1.1 | MOC: 2700W/ 3000VA |
| 1.2 | Topologia: on-line |
| 1.3 | Obudowa: Rack19” i Tower wys. 2U max gł. 608mm |
| 1.4 | Złącza wejściowe IEC C20: TAK |
| 1.5 | Czas autonomii bateryjnej: 7 min przy 75% |
| 1.6 | Zakres napięcia wejściowego AC: 120V – 276 VAC wejście nie przechodzi na pracę z baterii |
| 1.7 | Poziom hałasu (ba): ≤ 50 dB (A) |
| 1.8 | Zakres częstotliwości wejściowej: 45 – 66Hz |
| 1.9 | Regulacja napięcia: +/- 1% |
| 1.10 | Współczynnik Mocy: 0,9 |
| 1.11 | Kształt napięcia (wyjściowego): Sinusoida |
| 1.12 | Sprawność Tryb Liniowy: >92% |
| 1.13 | Sprawność Tryb Bateryjny: >86% |
| 1.14 | Panel kontrolny: LCD |
| 1.15 | Komunikaty z wyświetlacza: Stan UPS-a, częstotliwość napięcia wej. I wyj., poziom obciążenia, poziom i napięcia baterii. |
| 1.16 | Alarmy dźwiękowe: TAK |
| 1.17 | By-pass elektroniczny: TAK |
| 1.18 | Czas przełączenia liniowy << >> bateryjny: 0ms |
| 1.19 | Komunikacja: Slot na kartę SNMP: TAK |
| 1.20 | Złącze RS232: TAK |
| 1.21 | Złącze USB: TAK |
| 1.22 | Złącza IEC C13 10A: 8 / IEC C19 16A: 1 |
| 1.23 | Złącze DC do dodatkowych baterii: TAK |
| 1.24 | Możliwość uruchomienia z baterii: TAK |
| 1.25 | Automatyczny restart po powrocie napięcia: TAK |
| 1.26 | Oprogramowanie w języku Polskim: Windows, NT |
| 1.27 | Zakres temperatur pracy: 0 do 40°C |
| 1.28 | Wyposażenie: Kabel USB, szyny montażowe, uchwyty do montażu w szafie 19”, podstawki dla opcji TOWER |
| 1.29 | Gwarancja – minimum 24 miesiące |

**f) Skaner – szt. 4**

|  |  |
| --- | --- |
|  | **Opis wymaganych parametrów technicznych** |
| **1** | **2** |
| 1.1 | Format: A4 |
| 1.2 | Wyświetlacz: kolorowy ekran dotykowy |
| 1.3 | Waga skanera netto [kg] max. 4,6 kg |
| 1.4 | Zgodność z systemami operacyjnymi: Windows 10 (wersja 32 i 64 bitowa), Windows 8 (wersja 32 i 64 bitowa), Windows 7 (wersja 32 i 64 bitowa), Windows Vista, |
| 1.5 | Komunikacja: USB (3.0 SuperSpeed), Wireless, Ethernet, NFC |
| 1.6 | Parametry skanera:   * technologia skanowania: CIS (podwójny) * skanowanie w kolorze * optyczna rozdzielczość skanowania: do 600x600 dpi * rozszerzona rozdzielczość skanowania: do 1200x1200 dpi * szybkość skanowania: do 50 (str./min) * skanowanie dwustronne * kodowanie koloru: 24 bit * skala szarości: 256 poziomy * skanowanie do: email, plik, obraz, udział sieciowy, OCR, SharePoint, USB Host, FTP, |
| 1.7 | Obsługa nośników:   * gramatura nośników: od 27 g/m² do 413 g/m² * Automatyczny Podajnik Dokumentów * pojemność podajnika automatycznego: max. 50 arkuszy * niestandardowe wymiary nośników (szerokość) min 51 mm max 215,9 mm * niestandardowe wymiary nośników (długość) min 51 mm max 297 mm * obsługiwane rodzaje nośników: papier zwykły, papier o niskiej gramaturze, papier o wysokiej gramaturze, papier makulaturowy, wizytówki, karty plastikowe (tłoczone do 1,4 mm) * obsługiwane formaty nośników A4 |
| 1.8 | Kabel USB, ekranowany z ferytem |
| 1.9 | CD (zawiera oprogramowanie i podręcznik użytkownika) |
| 2.0 | Kabel zasilania |
| 2.1 | Gwarancja – minimum 24 miesiące |

**Część 2.**

**a) Aktualizacja oprogramowania antywirusowego na stacje robocze i serwery wraz z konsolą do centralnej administracji**

|  |
| --- |
| Aktualizacja licencji programu antywirusowego dla stacji roboczych – 290 szt.  Aktualizacja posiadanego przez zamawiającego oprogramowania ESET Endpoint Antivirus poprzez dostarczenie 290 licencji ww. oprogramowania lub oprogramowania równoważnego\*, uprawniających do pobierania w okresie jednego roku uaktualnień bazy danych wirusów programu użytkowanego przez zamawiającego (tzw. roczna subskrypcja aktualizacji bazy danych wirusów).  Aktualizacja licencji programu antywirusowego dla serwerów plikowych – 7 szt.  Aktualizacja posiadanego przez zamawiającego oprogramowania ESET File Security for Windows Server poprzez dostarczenie 7 licencji ww. oprogramowania lub oprogramowania równoważnego\*, uprawniających do pobierania w okresie jednego roku uaktualnień bazy danych wirusów programu użytkowanego przez zamawiającego (tzw. roczna subskrypcja aktualizacji bazy danych wirusów).  Zaoferowane oprogramowanie musi współpracować z wykorzystywanym przez zamawiającego centralnym serwerem zarządzającym oprogramowaniem ESET (Remote Administrator Server). Subskrypcja aktualizacji bazy danych wirusów dla ww. licencji ma obowiązywać przez rok od 19 listopada 2019 r.  Zamawiający dopuszcza zastosowanie innego, równoważnego\* rozwiązania pod warunkiem, że spełnia ono minimalne parametry przedstawione w poniższej specyfikacji:  **Stacje Windows (dotyczy również serwerów Windows)**  1. Pełne wsparcie dla systemu Windows Vista/Windows 7/ Windows 8/ Windows 10.  2. Wsparcie dla Windows Security Center (Windows XP SP2).  3. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.  4. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim.  5. Pomoc w programie (help) w języku polskim.  **Ochrona antywirusowa i antyspyware**   1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Wbudowana technologia do ochrony przed rootkitami. 3. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 4. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 5. 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. 6. 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 7. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 8. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 9. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 10. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. 11. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 12. 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. 13. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego). 14. 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). 15. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 16. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 17. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 18. 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. 19. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 20. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 21. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 22. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta. 23. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 24. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym. 25. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 26. 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. 27. 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. 28. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. 29. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła. 30. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. 31. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji. 32. 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. 33. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 34. 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 , urządzeń przenośnych oraz urządzeń dowolnego typu. 35. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. 36. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia. 37. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 38. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 39. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika 40. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 41. Oprogramowanie musi posiadać zaawansowany skaner pamięci. 42. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp. 43. 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. 44. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. 45. 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. 46. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. 47. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur. 48. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. 49. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http 50. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback). 51. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 52. Program ma być w pełni zgodny z technologią CISCO Network Access Control. 53. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji. 54. 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. 55. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 56. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.   **Ochrona serwera plików Windows**   1. Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016, SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012. 2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 4. Wbudowana technologia do ochrony przed rootkitami i exploitami. 5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 7. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 8. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. 9. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego. 10. Możliwość skanowania dysków sieciowych i dysków przenośnych. 11. Skanowanie plików spakowanych i skompresowanych. 12. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi. 13. Aplikacja powinna wspierać mechanizm klastrowania. 14. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 15. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. 16. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 17. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia. 18. 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. 19. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 20. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 21. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. 22. Dodanie automatycznych wyłączeń nie wymaga restartu serwera. 23. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. 24. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. 25. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione. 26. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego. 27. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). 28. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. 29. 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. 30. 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 będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. 31. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 32. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e‑mail. 33. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła. 34. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo. 35. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC. 36. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji. 37. Po instalacji systemu antywirusowego, 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. 38. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 39. System antywirusowy 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. 40. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. 41. System antywirusowy 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. 42. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP). 43. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 44. Aplikacja musi wspierać skanowanie magazynu Hyper-V 45. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów 46. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). 47. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 48. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.   **Administracja zdalna**   1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012 oraz systemach Linux. 2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). 3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL. 4. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta. 5. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. 6. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. 7. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający. 8. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL. 9. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. 10. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. 11. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny. 12. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym. 13. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. 14. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu. 15. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. 16. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy. 17. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci. 18. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. 19. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania. 20. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. 21. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika. 22. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play. 23. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. 24. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS. 25. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi. 26. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp. 27. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej 28. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji. 29. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. 30. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. 31. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany. 32. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji. 33. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym. 34. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu. 35. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką. 36. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów. 37. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp. 38. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta. 39. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej. 40. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku. 41. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania. 42. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie. 43. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW. 44. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS. 45. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego. 46. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. 47. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP. 48. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu. 49. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta. 50. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji. 51. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty. 52. Serwer administracyjny musi być wyposażona w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana. 53. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).   \* W przypadku zaoferowania oprogramowania równoważnego do posiadanego przez zamawiającego, celem potwierdzenia spełniania przez oferowane oprogramowanie wymagań określonych przez zamawiającego, wykonawca dołączy do oferty specyfikacje techniczne oferowanego oprogramowania.  Specyfikacje techniczne muszą być sporządzone w języku polskim. W przypadku dokumentów sporządzonych w języku obcym, wykonawca składa je wraz z tłumaczeniem na język polski, poświadczonym przez wykonawcę. |

**b) Dostawa oprogramowania do ochrony danych (szyfrowanie) – szt. 20**

* + - 1. Konsola centralnego zarządzania musi wspierać systemy operacyjne Microsoft Windows Server 2008 32-bit i 64-bit, 2012 64-bit, 2016 64-bit oraz Microsoft Windows 7/8/10 32-bit i 64-bit.
      2. Serwer centralnego zarządzania musi współpracować co najmniej z silnikami baz danych takimi jak Microsoft SQL Server 2005, 2008, 2012.
      3. Konsola centralnego zarządzania musi pozwalać na generowanie pakietów instalacyjnych dla stacji końcowych w formacie MSI.
      4. Komunikacja pomiędzy serwerem centralnego zarządzania, a serwerem proxy musi odbywać się na bezpiecznym porcie 443.
      5. Administrator musi mieć możliwość tworzenia i zarządzania wieloma kluczami szyfrującymi, opartymi o kilka algorytmów szyfrujących, co najmniej AES, 3DES, Blowfish.
      6. Administrator musi mieć możliwość tworzenia różnych użytkowników, mających dostęp do konsoli centralnego zarządzania wraz z możliwością przypisywania im różnych ról.
      7. Administrator musi mieć możliwość tworzenia dodatkowych ról, na podstawie opcji dostępnych w konsoli centralnego zarządzania.
      8. Logowanie do konsoli centralnego zarządzania powinno być objęte warunkami złożoności hasła.
      9. Musi istnieć możliwość konfiguracji złożoności hasła do konsoli centralnego zarządzania, w oparciu o przynajmniej:

a) ilość znaków,

b) czy hasło ma zawierać wielkie litery,

c) czy hasło ma zawierać małe litery,

d) czy hasło ma zawierać cyfry,

e) czy hasło ma zawierać znaki specjalne,

f ) okres ważności,

g) ilość nieudanych logowań.

10. Administrator musi mieć możliwość konfiguracji złożoności haseł dla użytkowników na stacjach roboczych.

11. Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:

a) ilość znaków,

b) czy hasło ma zawierać wielkie litery,

c) czy hasło ma zawierać małe litery,

d) czy hasło ma zawierać cyfry,

e) czy hasło ma zawierać znaki specjalne,

f ) okres ważności,

g) ilość nieudanych logowań,

h) możliwość zmiany hasła.

12. Konsola centralnego zarządzania musi gromadzić informacje o:

a) nazwach stacji roboczych, na których jest zainstalowany klient systemu szyfrowania danych,

b) dacie ostatniej modyfikacji ustawień klienta systemu szyfrowania danych,

c) dacie aktywacji klienta systemu szyfrowania danych,

d) statusu szyfrowania,

e) typie urządzenia na którym jest zainstalowany klient systemu szyfrowania danych,

f) stanie polityki,

g) wersji klienta systemu szyfrowania danych,

h) wersji systemu operacyjnego stacji roboczej,

i) użytkownikach uprawnionych do logowania do oprogramowania na stacji roboczej.

13. Konsola centralnego zarządzania musi pozwalać na wygenerowanie dla każdej zaszyfrowanej stacji płyty ratunkowej.

14. Konsola musi być dostępna z poziomu interfejsu WWW.

15. Administrator musi mieć możliwość zarządzania stacjami klienckimi, które mają dostęp do sieci Internet.

16. Administrator musi mieć możliwość konfiguracji automatycznego szyfrowania pełnej powierzchni dysku po wykonanej instalacji oprogramowania.

17. Konsola centralnego zarządzania musi posiadać możliwość automatycznej aktywacji licencji w ramach kont domenowych.

18. Administrator musi mieć możliwość wykonania poniższych czynności w sposób zdalny:

a) instalacji klienta na stacji,

b) zaszyfrowania/odszyfrowania stacji,

c) wygenerowania klucza aktywacyjnego dla użytkownika,

d) administrowania kluczami szyfrującymi,

e) administrowania użytkownikami, którzy mają dostęp do stacji,

f) administrowania profilem ustawień dla użytkowników,

g) administrowania profilem ustawień dla stacji roboczych,

h) wymuszenia zmiany hasła,

i) zarządzania wieloma organizacjami z poziomu jednej konsoli.

WYMAGANIA SYSTEMOWE APLIKACJI KLIENCKIEJ

1. System szyfrowania danych musi wspierać instalacje aplikacji klienckiej w środowisku Microsoft Windows Vista/7/8/10 32-bit i 64-bit oraz w środowiskach Microsoft Windows Server, 2008 32-bit i 64-bit, 2012 64-bit, 2016 64-bit.

2. System musi posiadać certyfikat FIPS 140-2 Level 1

WYMAGANIA DOTYCZĄCE UWIERZYTELNIANIA

1. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.

2. Aplikacja musi umożliwiać określenie, co najmniej 127 unikalnych użytkowników, którzy będą mieć dostęp do chronionej stacji roboczej na poziomie Pre-Boot.

3. Aplikacja musi umożliwiać przetrzymywanie, co najmniej 64 kluczy szyfrujących w jednym pęku kluczy (key file).

4. Dostęp do pliku klucza musi być chroniony przy pomocy hasła. Domyślnie wykorzystywane hasło musi być hasłem systemu Windows.

5. Administrator musi posiadać możliwość modyfikacji ekranu logowania (Pre-boot).

WYMAGANIA DOTYCZĄCE USTAWIEŃ APLIKACJI KLIENCKIEJ

1. Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.

2. Defragmentacja dysku nie może mieć negatywnego wpływu na system szyfrowania.

3. Aplikacja musi umożliwiać szyfrowanie nośników wymiennych w następujący sposób:

a) sektor po sektorze,

b) kontener.

4. Zaszyfrowany nośnik wymienny oraz nośnik CD/DVD może być odczytany na dowolnej stacji, na której nie ma zainstalowanego klienta systemu szyfrowania. Dostęp do takiego nośnika musi być możliwy po podaniu hasła.

5. Aplikacja musi pozwalać na szyfrowanie wiadomości e-mail wraz z załącznikami.

6. Aplikacja musi umożliwiać automatyczną deszyfrację otrzymywanych wiadomości e-mail.

7. Aplikacja musi pozwalać na szyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.

8. Zaszyfrowany tekst może być odczytany, za pomocą narzędzia, dostarczanego przez producenta, na stacji bez zainstalowanego klienta systemu szyfrowania.

9. Aplikacja musi umożliwiać wybór klucza szyfrującego (w przypadku posiadania wielu kluczy w pęku), który ma być używany w procesie szyfrowania.

10. Aplikacja musi umożliwiać wybór domyślnego klucza szyfrowania.

11. Aplikacja musi umożliwiać zaszyfrowanie pliku lub folderu z poziomu menu kontekstowego.

12. Możliwe jest utworzenie skrótów klawiszowych umożliwiających zaszyfrowanie/odszyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.

13. Aplikacja musi umożliwiać tworzenie wirtualnych partycji. Dostęp do takich partycji ma być

możliwy przy użyciu klucza szyfrującego lub hasła.

14. Aplikacja musi umożliwiać zdefiniowanie wielkości wirtualnej partycji, z dokładnością do 1MB.

15. Aplikacja musi umożliwiać tworzenie zaszyfrowanego archiwum. Dostęp do takiego archiwum ma być możliwy, przy użyciu klucza szyfrującego lub hasła.

16. Aplikacja musi umożliwiać trwałe usuwanie danych za pomocą poniższych algorytmów:

a) Guttman.

b) US Department of Defence 5220.22-M (8-306. /E).

c) US Department of Defence 5220.22-M (8-306. /E, CiE).

d) Kryptograficzne losowe dane liczbowe.

17. Aplikacja musi posiadać dedykowaną wtyczkę co najmniej dla klientów pocztowych MS Outlook 2003 lub nowszych, również dostępnych z poziomu Office 365.

18. Aplikacja musi umożliwiać automatyczne zalogowanie użytkownika do pęku klucza (key file) systemu szyfrowania danych po uruchomieniu systemu operacyjnego.

19. Aplikacja musi umożliwiać automatyczne wylogowanie z aplikacji w przypadku bezczynności użytkownika w systemie.

20. Aplikacja musi posiadać opcję automatycznego odpytywania serwerów producenta o dostępność nowszych wersji.

21. Użytkownik musi posiadać możliwość ręcznego sprawdzania czy dostępna jest nowsza wersja programu, z poziomu GUI.

WYMAGANIA DOTYCZĄCE SZYFROWANIA

1. Aplikacja musi dawać możliwość szyfrowania powierzchni dysku sektor po sektorze.

2. Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.

3. Aplikacja musi umożliwiać wstrzymanie procesu szyfrowania powierzchni dysku i jego wznowienie.

Proces szyfrowania danych powinien rozpocząć się od momentu, w którym został przerwany.

4. Aplikacja musi umożliwiać wstrzymanie procesu szyfrowania, w sytuacji gdy laptop nie jest

podłączony do zasilania. Proces szyfrowania musi zostać wznowiony automatycznie, po podłączeniu zasilacza.

5. Wymagane jest wykorzystanie kluczy szyfrujących, utworzonych przy użyciu jednego z poniższych algorytmów szyfrowania:

a) AES (Rijndael).

b) Blowfish.

c) Triple DES (3DES).

6. Aplikacja musi umożliwiać współpracę z dyskami SSD.

7. Aplikacja musi umożliwiać współpracę z dyskami sprzętowo szyfrowanymi, działającymi w technologii TCG OPAL.

8. Aplikacja musi umożliwiać szyfrowanie danych na komputerach z UEFI.

9. Administrator musi mieć możliwość sprawdzenia, przed zaszyfrowaniem całej powierzchni dysku, czy nie pojawią się problemy po ponownym uruchomieniu komputera.

10. Administrator musi mieć możliwość opcjonalnego szyfrowania niesystemowych partycji dysku.

WYMAGANIA DOTYCZĄCE SYTUACJI KRYTYCZNYCH

1. W przypadku utraty hasła, aplikacja musi umożliwiać Administratorowi odzyskanie dostępu do zaszyfrowanego dysku poprzez użycie zdefiniowanego wcześniej hasła administratora.

2. W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do

zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła,

wygenerowanego z poziomu konsoli centralnego zarządzania.

Licencja bezterminowa

Aplikacja musi być objęta serwisem producenckim przez okres min. 12 miesięcy, polegającym na dostępie do aktualizacji oprogramowania oraz wsparciu technicznym w trybie 8x5 - w dni robocze od poniedziałku do piątku, w godzinach pracy od 7.30-15.30.

**Część 3.**

Dostawa komputerów typu laptop wraz z oprogramowaniem systemowym i wyposażeniem – 5 szt. Dostawa oprogramowania biurowego – 5 szt.

|  |  |
| --- | --- |
|  | **Opis wymaganych parametrów technicznych** |
| **1** | **2** |
| 1.1 | Typ: laptop |
| 1.2 | Procesor: wielordzeniowy klasy x86, osiągający według testu PassMark Average CPU Mark wynik min. 5350 punktów.  *Zamawiający wezwie Wykonawcę, którego oferta zostanie najwyżej oceniona  do złożenia wydruku ze strony http://www.cpubenchmark.net potwierdzającego spełnianie wymagań dla zaoferowanego urządzenia, z datą nie później niż na dzień składania ofert.* |
| 1.3 | Pamięć: nie mniej niż 8 GB SO-DIMM DDR4, gniazda na pamięć (ogółem/wolne) 2/1 |
| 1.4 | Dysk twardy SSD min. 256 GB |
| 1.5 | Płyta główna: częstotliwość pracy magistrali FSB – zgodna z oferowanym modelem procesora |
| 1.6 | Przekątna ekranu: 15,6” |
| 1.7 | Typ ekranu: LED, Matowy |
| 1.8 | Rozdzielczość ekranu: 1920x1080 (FullHD) |
| 1.9 | Zintegrowana karta graficzna: Tak |
| 1.10 | Zintegrowana karta dźwiękowa: Tak |
| 1.11 | Łączność:  Wi-Fi 802.11 b/g/n/ac  Moduł Bluetooth  LAN 10/100/1000 Mbps |
| 1.11 | Interfejsy:  USB 3.1 Gen. 1 (USB 3.0) – min.2 szt.  USB 2.0 – min.1 szt.  HDMI – 1 szt.  Czytnik kart pamięci - 1 szt.  Wyjście słuchawkowe/wejście mikrofonowe - 1 szt.  RJ-45 (LAN) - 1 szt.  DC-in (wejście zasilania) - 1 szt. |
| 1.12 | Bateria: 3-komorowa, min. 3500 mAh, Li-Ion |
| 1.13 | Zasilacz: Tak |
| 1.14 | Waga: do 2 kg (z baterią) |
| 1.15 | System operacyjny: Microsoft Windows 10 Pro PL (wersja 64-bitowa) lub równoważny.  Warunki równoważności: System operacyjny 64-bit, dołączony nośnik z oprogramowaniem. Za rozwiązanie równoważne uznaje się takie, które posiada wbudowane mechanizmy, bez użycia dodatkowych aplikacji (bez jakichkolwiek emulatorów, implementacji lub programów towarzyszących), zapewniające:  1. polską wersję językową,  2. możliwość instalacji i poprawnego działania oprogramowania dostępnego w ramach posiadanych przez Zamawiającego licencji Microsoft Office 2010, Microsoft Office 2013, Microsoft Office 2016) oraz możliwość pełnej integracji z systemem domenowym MS Windows,  3. możliwość instalacji i poprawnego działania aplikacji wykorzystywanych przez Zamawiającego, oraz poprawnej obsługi powszechnie używanych, urządzeń peryferyjnych (drukarek, skanerów, kser), 4. dostępność aktualizacji i poprawek do systemu u producenta systemu bezpłatnie i bez dodatkowych opłat licencyjnych z możliwością wyboru instalowanych poprawek,  5. możliwość zdalnej, automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu,  6. możliwość automatycznego zbudowania obrazu systemu wraz z aplikacjami, obraz systemu służyć ma do automatycznego upowszechniania systemu operacyjnego inicjowanego i wykonywanego w całości przez sieć komputerową,  7. możliwość wdrożenia nowego obrazu przez zdalną instalację,  8. graficzne środowisko instalacji i konfiguracji,  9. możliwość udostępniania i przejmowania pulpitu zdalnego,  10. możliwość udostępniania plików i drukarek,  11. możliwość blokowania lub dopuszczenia dowolnych urządzeń peryferyjnych za pomocą polityk sprzętowych (np. przy użyciu numerów identyfikacyjnych sprzętu),  12. zapewnienie wsparcia dla większości powszechnie używanych urządzeń (drukarek, urządzeń sieciowych, standardów USB, urządzeń Plug & Play, WiFi,  13. wyposażenie systemu w graficzny interfejs użytkownika w języku polskim,  14. zapewnienie pełnej kompatybilności z oferowanym sprzętem,  15. zintegrowanie z systemem modułu pomocy dla użytkownika w języku polskim,  16. zintegrowanie z systemem modułu wyszukiwania informacji,  17. możliwość wykonywania kopii bezpieczeństwa (całego dysku, wybranych folderów, kopii przyrostowych) wraz z możliwością automatycznego odzyskania wersji wcześniejszej,  18. zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników,  19. zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacja dostępna u producenta nieodpłatnie bez ograniczeń czasowych,  20. licencja na system operacyjny musi być nieograniczona w czasie, pozwalać na wielokrotne instalowanie systemu na oferowanym sprzęcie bez konieczności kontaktowania się przez Zamawiającego z producentem systemu lub sprzętu,  21. oprogramowanie powinno pochodzić z legalnego źródła i posiadać certyfikat autentyczności lub unikalny kod aktywacyjny nieużywany oraz nieaktywowany nigdy wcześniej na innym urządzeniu,  22. zamawiający nie dopuszcza w systemie możliwości instalacji dodatkowych narzędzi emulujących działanie systemów.  W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania |
| 1.16 | Oprogramowanie Microsoft Office 2019 Home and Business 2019 PL lub rozwiązanie równoważne.  Warunki równoważności:  Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej,  Wymagania odnośnie interfejsu użytkownika:  a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.  b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.  c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.  Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi katalogowej Active Directory.  Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.  Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:  a. posiada kompletny i publicznie dostępny opis formatu,  b. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012, poz. 526),  c. umożliwia kreowanie plików w formacie XML,  d. wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,  Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.  W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).  Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.  Pakiet zintegrowanych aplikacji biurowych musi zawierać:  a. Edytor tekstów  b. Arkusz kalkulacyjny  c. Narzędzie do przygotowywania i prowadzenia prezentacji  d. Narzędzie do tworzenia drukowanych materiałów informacyjnych  e. Narzędzie do tworzenia i pracy z lokalną bazą danych  f. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)  g. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.  h. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.  Edytor tekstów musi umożliwiać:  a. 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.  b. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.  c. Wstawianie oraz formatowanie tabel.  d. Wstawianie oraz formatowanie obiektów graficznych.  e. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).  f. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.  g. Automatyczne tworzenie spisów treści.  h. Formatowanie nagłówków i stopek stron.  i. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.  j. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.  k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.  l. Określenie układu strony (pionowa/pozioma).  m. Wydruk dokumentów.  n. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.  o. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.  p. Zapis i edycję plików w formacie PDF.  q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  r. Możliwość jednoczesnej pracy wielu użytkowników na jednym dokumencie z uwidacznianiem ich uprawnień i wyświetlaniem dokonywanych przez nie zmian na bieżąco,  s. Możliwość wyboru jednej z zapisanych wersji dokumentu, nad którym pracuje wiele osób.  Arkusz kalkulacyjny musi umożliwiać:  a. Tworzenie raportów tabelarycznych  b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych  c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.  d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)  e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych  f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych  g. Wyszukiwanie i zamianę danych  h. Wykonywanie analiz danych przy użyciu formatowania warunkowego  i. Tworzenie wykresów prognoz i trendów na podstawie danych historycznych z użyciem algorytmu ETS  j. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie  k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności  l. Formatowanie czasu, daty i wartości finansowych z polskim formatem  m. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.  n. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.  o. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj wykresu).  p. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013 i 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.  q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji  Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:  a. Przygotowywanie prezentacji multimedialnych, które będą:  b. Prezentowanie przy użyciu projektora multimedialnego  c. Drukowanie w formacie umożliwiającym robienie notatek  d. Zapisanie jako prezentacja tylko do odczytu.  e. Nagrywanie narracji i dołączanie jej do prezentacji  f. Opatrywanie slajdów notatkami dla prezentera  g. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo  h. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego  i. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym  j. Możliwość tworzenia animacji obiektów i całych slajdów  k. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu.  l. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016.  Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:  a. Tworzenie i edycję drukowanych materiałów informacyjnych  b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.  c. Edycję poszczególnych stron materiałów.  d. Podział treści na kolumny.  e. Umieszczanie elementów graficznych.  f. wykorzystanie mechanizmu korespondencji seryjnej  g. Płynne przesuwanie elementów po całej stronie publikacji.  h. Eksport publikacji do formatu PDF oraz TIFF.  i. Wydruk publikacji.  j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.  Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać:  a. Tworzenie bazy danych przez zdefiniowanie:  b. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.  c. Relacji pomiędzy tabelami  d. Formularzy do wprowadzania i edycji danych  e. Raportów  f. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych  g. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów  h. Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.  Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:  a. Uwierzytelnianie wieloskładnikowe poprzez wbudowane wsparcie integrujące z usługą Active Directory,  b. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,  c. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,  d. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,  e. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,  f. Automatyczne grupowanie poczty o tym samym tytule,  g. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,  h. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,  i. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,  j. Zarządzanie kalendarzem,  k. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,  l. Przeglądanie kalendarza innych użytkowników,  m. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,  n. Zarządzanie listą zadań,  o. Zlecanie zadań innym użytkownikom,  p. Zarządzanie listą kontaktów,  q. Udostępnianie listy kontaktów innym użytkownikom,  r. Przeglądanie listy kontaktów innych użytkowników,  s. Możliwość przesyłania kontaktów innym użytkowników,  t. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.  Oprogramowanie powinno pochodzić z legalnego źródła i posiadać certyfikat autentyczności lub unikalny kod aktywacyjny nieużywany oraz nieaktywowany nigdy wcześniej na innym urządzeniu.  Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu.  Okres licencji: Bezterminowa |
| 1.17 | Dołączone wyposażenie do każdego laptopa: |
| Mysz optyczna, rolka, standard – USB |
| Torba |
| 1.18 | Gwarancja – min.24 miesięcy |

**Część 4.**

* 1. **Dostawa, wdrożenie i serwis urządzeń UTM**

1. Wymagania Ogólne
2. Oferowane produkty muszą spełniać obowiązujące normy i parametry dopuszczające je do sprzedaży oraz używania na terenie Polski oraz krajów UE, posiadać znak zgodności CE.
3. Oferowane produkty muszą być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostawy, nieużywane i gotowe do pracy bez żadnych dodatkowych zakupów czy inwestycji.
4. Wykonawca winien przedstawić nazwę producenta i model oferowanego produktu i oprogramowania w poszczególnych jego rodzajach.
5. Wykonawca musi dostarczyć oferowany produkt z niezbędnym okablowaniem.
6. Oferowany produkt musi współdziałać z posiadanymi przez Zamawiającego urządzeniami FortiGate 200E.
7. 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. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

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, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

• Firewall

• Ochrony w warstwie aplikacji

• Protokołów routingu dynamicznego.

1. Redundancja, monitoring i wykrywanie awarii

a) 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 powinna istnieć funkcja synchronizacji sesji firewall.

b) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

c) Monitoring stanu realizowanych połączeń VPN.

4. Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum 7 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 32 GB.
5. System musi być wyposażony w zasilanie AC.

5. Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 1.8 mln jednoczesnych połączeń oraz 21.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 2.5 Gbps.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 450 Mbps.
4. Wydajność szyfrowania IPSec VPN: nie mniej niż 90 Mbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 350 Mbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 160 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 150 Mbps.

6. Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.

7. Polityki, Firewall

Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

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.

W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

1. Połączenia VPN

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, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.

• 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 (np. OSPF) 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 Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

9. Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   * Routingu statycznego.
   * Policy Based Routingu.
   * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

10. Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

11. Kontrola Antywirusowa

Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

12. Ochrona przed atakami

Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

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.

Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

13. Kontrola aplikacji

Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

14. Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

15. Uwierzytelnianie użytkowników w ramach sesji

a) 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 (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

16. Zarządzanie

Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

17. Logowanie

Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

Musi istnieć możliwość logowania do serwera SYSLOG.

18. Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

• ICSA lub EAL4 dla funkcji Firewall.

• ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.

• CSA dla funkcji SSL VPN.

19. Licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [36] miesięcy.

20. Gwarancja i serwis

Urządzenia UTM muszą być objęte serwisem producenckim przez okres min. 36 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 8x5 - w dni robocze od poniedziałku do piątku, w godzinach pracy od 7.30-15.30.

Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez moduł internetowy oraz infolinię w języku polskim. Wykonawca winien przedłożyć dokumenty:

• Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).

21. Zakres wdrożenia systemu firewalli w Wojewódzkim Urzędzie Pracy w Poznaniu oraz oddziałach zamiejscowych w Kaliszu, Koninie, Lesznie, Pile:

1. weryfikacja ilościowa i jakościowa dostarczanego sprzętu
2. montaż urządzeń firewall w wyznaczonych punktach oddziałów zamiejscowych
3. podłączenie firewalli do istniejącej infrastruktury sieciowej
4. wyrównanie wersji oprogramowania na wszystkich urządzeniach w WUP w Poznaniu i oddziałach zamiejscowych
5. konfiguracja istniejącego klastra firewall zlokalizowanego w WUP w Poznaniu w zakresie:

• tuneli IPSec VPN do oddziałów zamiejscowych

• polityk dostępowych dla ruchu z oddziałów zamiejscowych

• dynamicznego protokołu routingu OSPF

1. konfiguracja firewalli w oddziałach zamiejscowych w zakresie:

• profili zabezpieczających (antywirus, filtr stron internetowych, kontrola aplikacji, IPS) zgodnie z dobrymi praktykami i wymaganiami klienta

• autoryzacji użytkowników za pomocą SSO

• tuneli IPSec VPN do WUP w Poznaniu

• polityk dostępowych do Internetu i ruchu do Urzędu

• tuneli IPSec VPN do Urzędu

• dynamicznego protokołu routingu OSPF

1. przeprowadzenie testów poprawności działania połączeń z oddziałów do Internetu i WUP w Poznaniu
2. wykonanie opisu wdrożenia

22. Wykaz osób, które będą wykonywać zamówienie:

W związku z posiadanymi przez zamawiającego jednostkami FortiGate 200E zamawiający wymaga wykazania dysponowaniem odpowiednim potencjałem technicznym, tj. min. dwoma akredytowanymi inżynierami w tym min. 1 na poziomie min. NSE8 oraz 1 na poziomie min. NSE4

1. **dostawa macierzy dyskowej wraz z usługą instalacji, konfiguracji i migracji danych**

|  |  |
| --- | --- |
| **Komponent** | **Minimalne wymagania** |
| Wymagania Ogólne | 1. Oferowany produkt musi spełniać obowiązujące normy i parametry dopuszczające go do sprzedaży oraz używania na terenie Polski oraz krajów UE, posiadać znak zgodności CE. 2. Oferowany produkt musi być fabrycznie nowy, wyprodukowany nie wcześniej niż 6 miesięcy przed datą dostawy, nieużywany i gotowy do pracy bez żadnych dodatkowych zakupów czy inwestycji. 3. Wykonawca winien przedstawić nazwę producenta i model oferowanego produktu i oprogramowania w poszczególnych jego rodzajach. 4. Wykonawca musi dostarczyć oferowany produkt z niezbędnym okablowaniem. |
| Zasoby dyskowe | 1. Macierz dyskowa musi być dostarczona z minimum:   * 5 dyskami SSD 2,5” o pojemności minimum 400GB, * 5 dyskami SAS 10k 2,5” o pojemności minimum 1,8TB   2. Macierz dyskowa musi mieć możliwość podłączenia dodatkowych dysków twardych o parametrach:   * dyski SSD o pojemności minimum 3.2TB oraz * dyski NL\_SAS 7,2k o pojemności minimum 6TB   3. Macierz musi mieć możliwość utworzenia grupy RAID w której dwa dyski, które będą przechowywać dane parzystości.  4. Awaria dwóch dowolnych dysków w obrębie takiej pojedynczej grupy RAID nie może spowodować utraty danych.  5. Kontrolery macierzy dyskowej muszą obsługiwać minimum 250 dysków oraz pojemność surową minimum 2PB, musi być możliwość rozbudowy podczas ciągłego dostępu hostów do danych do minimum 500 dysków.  6. Należy dodatkowo dostarczyć dyski zapasowe lub pojemność zapasową w ilości zgodnej z zaleceniami producenta dla oferowanej konfiguracji – nie mniej niż 1 zapasowy dysk lub jego pojemność na 30 dysków danego typu.  7. Podczas awarii dysku kontroler macierzy dyskowej musi automatycznie rozpoczynać odtwarzanie danych na fizycznym dysku zapasowym lub pojemności zapasowej.  8. W przypadku stosowania dysku zapasowego proces odtwarzania danych nie może wiązać się z procesem przenoszenia danych po wymianie dysku uszkodzonego (dysk wymieniony musi być automatycznie uznany za zapasowy). |
| Kontrolery macierzy dyskowej | 1. Macierz dyskowa musi być złożona z minimum jednej pary identycznych kontrolerów tworzących klaster wysokiej dostępności (high availability cluster). Kontrolery muszą udostępniać dane poprzez iSCSI, FCP, CIFS oraz NFS.  2. Obszar pamięci cache przeznaczony do zapisów danych, musi posiadać lustrzaną kopię (ang. mirror).  3. W przypadku awarii zasilania dane nie zapisane na dyskach muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub zachowane w pamięci nieulotnej kontrolera do momentu przywrócenia zasilania.  4. Kontrolery w klastrze wysokiej dostępności muszą oferować funkcjonalność automatycznego przejmowania funkcjonalności i zadań w przypadku awarii drugiego kontrolera w tej samej parze.  5. Macierz musi mieć minimum 256GB pamięci cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy. Włączenie lub wyłączenie pamięci cache nie może wymagać operacji usunięcia i utworzenia na nowo wolumenów lub grup dyskowych.  6. System operacyjny kontrolerów musi natywnie obsługiwać automatyczny tiering bloków danych pomiędzy dyskami SSD, SAS, NL\_SAS (macierz może alokować bloki dla danego wolumenu spośród wszystkich typów dysków: SSD, SAS, NL\_SAS równocześnie).  7. Macierz musi mieć możliwość obsługi różnych poziomów RAID równocześnie. Minimum RAID 1 (lub 10), 5, 6. Macierz musi umożliwiać konstrukcję urządzenia LUN w taki sposób, aby zawierał dane zabezpieczone poziomami RAID 1 (lub 10), RAID 5, RAID 6 jednocześnie.  8. Awaria dowolnego pojedynczego aktywnego elementu macierzy dyskowej nie może powodować przerwy w dostępie do danych.  9. Musi być możliwe utworzenie minimum 1000 wolumenów blokowych o rozmiarze minimum 256TB i plikowych o rozmiarze minimum 256TB.  10. Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości. |
| Interfejsy | Macierz musi być wyposażona w następujące działające porty:   * 4 porty 10GbaseT do podłączania hostów * 4 porty FC 16Gb do podłączania hostów – porty muszą być obsadzone odpowiednimi wkładkami SFP+ SR * 2 porty 1GbE Base-T do zdalnego zarządzania kontrolerem * 4 porty SAS minimum 12Gbs do podłączania półek dyskowych   Porty przeznaczone do podłączenia hostów nie mogą być wykorzystane do połączeń wewnątrz macierzy (np. pomiędzy kontrolerami).  Musi być możliwość rozbudowy on-line macierzy o minimum 16 portów (FC 16Gb lub 10Gb SFP+ lub 10GBaseT) jedynie poprzez instalację dodatkowych kart rozszerzeń bez konieczności instalacji dodatkowych kontrolerów. |
| Kopie migawkowe | 1.System operacyjny macierzy dyskowej musi natywnie obsługiwać mechanizm kopii migawkowych, który będzie dostępny dla wszystkich rodzajów danych udostępnianych. Niedopuszczalne są rozwiązania wykonujące kopie migawkowe jedynie w trybie Copy On Write dla dowolnego rodzaju danych (blokowe lub plikowe). Licencja na wszystkie opisane funkcjonalności musi obejmować całą powierzchnię użytkową macierzy.  2. Odtwarzanie plików i folderów z kopii migawkowych wykonanych dla wolumenów plikowych udostępnionych dla systemów typu Windows i Unix musi być dostępne za pomocą wydzielonego udziału sieciowego z zachowaniem praw dostępu na poziomie użytkownika.  3. System operacyjny macierzy dyskowej musi umożliwiać i wykonywanie kopii migawkowych wolumenów plikowych, w trybie on-line, bez zatrzymywania operacji odczytu i zapisu. Deklarowana przez producenta liczba kopii migawkowych musi wynosić minimum 256 na wolumen.  4. Musi być możliwe odtwarzanie danych z kopii migawkowych bezpośrednio na wolumen produkcyjny.  5. Musi być możliwe zaprezentowanie kopii migawkowej w trybie do odczytu i zapisu. |
| Obsługiwane protokoły | 1.System operacyjny macierzy dyskowej musi udostępniać dane za pomocą protokołu CIFS i FCP - jeśli do uruchomienia potrzebna jest licencja to zamawiający wymaga jej dostarczenia. System operacyjny macierzy dyskowej musi mieć możliwość uruchomienia udostępniania danych za pomocą protokołów NFS oraz iSCSI - licencje na protokoły CIFS, NFS, FCP oraz iSCSI są przedmiotem obecnego postępowania.  2. Jednoczesna obsługa różnych protokołów dostępu do danych nie może być zrealizowana za pomocą dodatkowego oprogramowania ani dodatkowych urządzeń pośredniczących typu wirtualizator, gateway, switch, etc. firm trzecich. |
| Pozostałe wymagania | 1. System operacyjny macierzy dyskowej musi umożliwiać dynamiczną zmianę rozmiaru wolumenów danych: (zwiększanie) bez przerywania pracy i bez przerywania użytkownikom zewnętrznym dostępu do danych  2. Musi być możliwość konfiguracji macierzy dyskowej za pomocą GUI, zbieranie i wyświetlanie informacji o stanie zasobów macierzy dyskowej, prezentowanie i gromadzenie zdarzeń zachodzących w macierzy dyskowej oraz prezentowanie bieżących statystyk wydajnościowych macierzy dyskowej, podgląd parametrów wydajnościowych macierzy dyskowej w czasie rzeczywistym.  3. Dostęp do CLI systemu operacyjnego kontrolerów musi odbywać się przy użyciu połączenia szyfrowanego.  4.W systemie operacyjnym kontrolera musi być możliwość utworzenia wirtualnych serwerów plików, a każdy wirtualny serwer plików musi obsługiwać użytkowników z innej domeny Microsoft [MS Active Directory).  5. W celu zabezpieczania danych macierz dyskowa musi mieć możliwość replikacji jej zasobów na zasoby innej macierzy tej samej rodziny. Replikacja musi działać na poziomie systemu operacyjnego macierzy i pracować w trybie asynchronicznym bez potrzeby użycia urządzeń zewnętrznych typu gatawey, serwer pośredniczący, etc. Musi istnieć możliwość odwrócenia kierunku replikacji. Replikacja danych między macierzami nie może być zrealizowana zewnętrznym narzędziem software'owym. Licencja na replikację jest przedmiotem obecnego postępowania.  6. System operacyjny kontrolerów macierzy musi oferować funkcjonalność QoS (Quality of Service) dla dowolnego wolumenu blokowego, to znaczy musi być możliwość ograniczenia liczby operacji na sekundę lub przepustowości w kB (lub analogicznych jednostkach) na sekundę, jaka jest możliwa do uzyskania ze wskazanego przez administratora wolumenu. |
| Wymiana dysków | Wymiana dysków może być dokonywana przez Zamawiającego. |
| Gwarancja | Urządzenie musi być objęte serwisem producenckim przez okres 36 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 8x5 - w dni robocze od poniedziałku do piątku, w godzinach pracy od 7.30-15.30. |
| Usługa instalacji, konfiguracji i migracji danych | 1. Macierz dyskowa musi być dostarczona do siedziby zamawiającego i zainstalowana we wskazanej przez Zamawiającego szafie RACK.  2. W ramach instalacji Wykonawca musi dokonać aktualizacji oprogramowania zainstalowanego na macierzy dyskowej do najnowszej dostępnej wersji, skonfigurować grupy RAID, wykonać rekonfigurację połączeń w sieci SAN, wykonać instalację niezbędnego okablowania oraz dokonać wszystkich prac związanych z migracją danych z macierzy produkcyjnej na nową macierz. |

**Część 5.**

1. Usługa serwisu pogwarancyjnego producenta sprzętu - HPE 1 year post warranty Foundation Care Next business day DL360p Gen8 Service dwóch serwerów HP DL360p Generacja 8, nr seryjne CZ3332KV9Y i CZ3332KVA1

* Czas trwania – 1 rok począwszy od dnia 21.11.2019 r.
* Metoda usługi - sprzęt w siedzibie klienta
* Odpowiedź - reakcja w następnym dniu roboczym z uwzględnieniem standardów HP
* Okres obowiązywania - standardowe dni i godziny pracy

1. Usługa serwisu producenckiego na okres 3 lat:

- CON-SNT-2901SEC dla routera CISCO C2901-VSEC/K9 – 3 szt.

- CON-SNT-2921 dla routera CISCO C2921-VSEC/K9 – 1 szt.

- CON-SNT-2951 dla routera CISCO C2951-VSEC/K9 – 1 szt.

* Czas trwania – 3 lata począwszy od dnia podpisania umowy
* naprawa lub wymiana sprzętu w trybie „następny dzień roboczy” od dnia zgłoszenia,
* dostęp do narzędzi i bazy wiedzy Cisco,
* bezpośredni dostęp do Technical Support – wsparcia technicznego Cisco, dostępne dla Urzędu poprzez telefon lub email (Service Request).
* Okres obowiązywania - standardowe dni i godziny pracy