**Załącznik nr 6 do SWZ**

**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: 43 szt.**

|  |  |
| --- | --- |
|  | **Opis wymaganych parametrów technicznych** |
| **1** | **2** |
| 1.1 | Typ: stacjonarny All in One |
| 1.2 | Wydajność: Komputer osiągający ogólny wynik min.1590 pkt w teście Bapco Sysmark 2018 oraz wynik dla testów składowych Overall Rating: Productivity  min. 1410 punktów  Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta. |
| 1.3 | Pamięć: 1 x min. 8GB, 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  - 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/ax  Bluetooth min 4.2 |
| 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 (z przodu ) * kamera internetowa min. 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  przyciski umożliwiające regulację jasności obrazu oraz wybór źródła obrazu |
| 1.11 | Zasilacz: aktywny stabilizator PFC, moc min. 90W |
| 1.12 | Obudowa typu All in One – zintegrowany komputer w obudowie wraz z monitorem z matrycą IPS min 23,8” o parametrach:  - rozdzielczość 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/+20 stopni (+/-1 stopień)  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 ( klucz systemu zaszyty w bios ) 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 2013, Microsoft Office 2016 i Microsoft Office 2019) 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, układ polski programisty |
| Mysz optyczna, rolka, standard – USB |
| 1.18 | Certyfikaty i standardy: |
| Certyfikat jakości ISO 9001: 2000 producenta komputera |
| Komputery posiada oprogramowanie producenta, które będzie umożliwiało rozpoznanie modelu i numeru seryjnego komputera, aktualizację sterowników oraz narzędzie diagnostyczne i do rozwiązywania problemów. |
| 1.19 | Gwarancja – min.36 miesięcy |

**b) Drukarka laserowa mono – szt. 5**

|  |  |
| --- | --- |
|  | **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 | Maksymalna pojemność pamięci [MB] – 256 |
| 1.6 | Szybkość procesora – 1500 MHz |
| 1.7 | Waga drukarki [kg] max. 12 kg |
| 1.8 | Głośność: Poziom mocy akustycznej: maksymalni 4,0 B(A)  Ciśnienie akustyczne: LpAm maksymalnie 54 dB(A) |
| 1.9 | Pojemność podajnika standardowego [arkusze] – min.100 |
| 1.10 | Pojemność podajnika kasety głównej [arkusze] – min.550 |
| 1.11 | Obsługiwane formaty nośników: A4, A5, A6, B5 |
| 1.12 | Panel sterowania:  wyświetlacz LCD, |
| 1.13 | Maksymalne zużycie: 780 W (aktywność), 14,5 W (oczekiwanie), 8,5 W (tryb Powersave), 0,6 W (urządzenie wyłączone) |
| 1.14 | 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.) |
| 1.15 | Obsługiwane gramatury nośników:  od 60 do 220 g/m² |
| 1.16 | Łączność:  Szybkie porty Host/Device USB 2.0 Interfejs Fast Ethernet 10Base-T/100Base-TX, Gigabit Ethernet 1000Base-T |
| 1.17 | Języki opisu strony/emulacje:  PCL 5, PCL 6, Postscript Level 3, PDF |
| 1.18 | Kabel USB, ekranowany z ferrytem |
| 1.19 | Materiały eksploatacyjne:  Toner dostarczany jako pojedynczy kartridż |
| 1.20 | CD (zawiera oprogramowanie i podręcznik użytkownika) lub oprogramowanie i podręcznik użytkownika do pobrania z dedykowanej przez producenta strony internetowej. |
| 1.21 | Kabel zasilania |
| 1.22 | Gwarancja – minimum 12 miesiące |

* 1. **Małe kolorowe urządzenie wielofunkcyjne – 1 szt.**

|  |  |
| --- | --- |
|  | **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, 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: min. 30 str./min * Wydruk pierwszej strony w czerni, A4, po wyjściu ze stanu gotowości: max. 10,5 s * Jakość druku w czerni i kolorze – min. 600x600 dpi * 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): min.19,5 str./min w czerni, min. 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: min. 30 kopii/min * Rozdzielczość kopii w czerni i kolorze: min. 300 x 300 dpi |
| 2.2 | Faksowanie:  Prędkość przesyłania faksu: 33,6 kb/s  Pamięć faksu: min. 250 stron  Rozdzielczość faksu w czerni: min. 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) lub oprogramowanie i podręcznik użytkownika do pobrania z dedykowanej przez producenta strony internetowej. |
| 2.5 | Kabel zasilania |
| 2.6 | Gwarancja – minimum 12 miesięcy |

* 1. **zakup dysków zewnętrznych – 3 szt.**

|  |  |
| --- | --- |
|  | **Opis wymaganych parametrów technicznych** |
| **1** | **2** |
| 1.1 | Rodzaj: zewnętrzny |
| 1.2 | Pojemność: 2 TB |
| 1.3 | Format: 2,5" |
| 1.4 | Rodzaj podłączenia: USB 3.0 i USB 2.0 |
| 1.5 | Dodatkowo: wstrząsoodporny, odporny na zarysowania |
| 1.6 | Waga: max 390 g |
| 1.7 | Zasilanie: USB |
| 1.8 | Gwarancja: 36 miesięcy |

* 1. **Oprogramowanie do wideokonferencji – 9 szt.**

1. Liczba licencji: 9, licencja roczna
2. Możliwość przyłączenia do 100 osób
3. Bez ograniczeń czasowych dla spotkań 1:1
4. Ograniczony czas spotkań grupowych do 24 godzin
5. Możliwość przyłączenia się do spotkania z dowolnego urządzenia: PC, laptop, smartfon (Mac, Windows, Linux, iOS i Android)
6. Kontrola uczestników przez prowadzącego w zakresie udostępniania wideo, dźwięku i ekranu
7. Czat grupowy
8. Zarządzanie uczestnikami, możliwość przydzielania ról na spotkaniu
9. Transmisja szyfrowana za pomocą Secure Socket Layer (SSL) oraz Advanced Encryption Standard (AES) 256-bit algorytmu.
10. Pełne szyfrowanie e2e pomiędzy nadawcą i adresatami komunikacji
11. Zaawansowane funkcje zarządzania spotkaniem: czat, szyfrowanie, powiadomienia
12. Analizy i podsumowanie spotkań: liczba spotkań, uczestników, terminy i czas ich trwania
13. Spersonalizowany identyfikator dla spotkań, tzw. ID
14. Domyślne włączanie hasła do spotkań
15. Możliwość włączenia funkcji poczekalni
16. Blokowanie możliwości dołączania nieznanych uczestników
17. W przypadku przetwarzania danych osobowych zapewnienie ich ochrony i bezpieczeństwa zgodnie z zasadami określonymi w RODO
    1. **Oprogramowanie do szyfrowania danych – 40 szt.**
       * 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

* 1. **rozszerzenie z 220 do 235 licencji oprogramowania Statlook w wersji 14, lub rozwiązanie równoważne.**

1. Rozszerzenie z 220 do 235 licencji oprogramowania Statlook w wersji 14 lub równoważnego oprogramowania w zakresie następujących funkcji:
2. Zarządzanie zasobami:

* Pozyskiwanie informacji o sprzęcie
* Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania
* Zdalne wykrywanie urządzeń w sieci za pomocą protokołów PING, ARP oraz SNMP
* Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu Operacyjnego wraz z informacją o aktualizacji
* Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy
* Odwzorowanie struktury organizacji w oparciu o Active Directory
* Jednostronna synchronizacja komputerów z AD (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory)
* Grupowanie wyposażenia z podziałem na jednostki organizacyjne w firmie
* Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.)
* Utworzenie własnych typów elementów wyposażenia
* Łączenie elementów wyposażenia w zestawy
* Przypisywanie zasobu do wielu zestawów
* Makrodefinicje w celu spersonalizowania nazw elementów w drzewku wyposażenia
* Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach
* Podpięcie dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików
* Przypisywanie sprzętu do konkretnych osób
* Przypisywanie sprzętu do wybranej firmy
* Automatyczne wyznaczanie 'Głównego użytkownika' komputera
* Wiązanie wielu rekordów wyposażenia z użytkownikiem
* Przypisywanie sprzętu do dowolnej lokalizacji
* Definiowanie własnych, dowolnych atrybutów sprzętu
* Grupowa zmiana domeny/grupy roboczej zasobu

1. Informacje o sprzęcie

* Automatyczne wykrywanie typu komputera (Desktop\Notebook\Serwer\Kontroler domeny) na podstawie wyników skanowania sprzętu
* Wykrywanie komputerów typu All-In-One
* Automatyczne wykrywanie typów stacji roboczej (Tower\Desktop\SFF\uSFF)
* Automatyczne uzupełnianie informacji o procesorze, liczbie rdzeni, ilości pamięci RAM, rozmiarze dysku, nazwie karty graficznej i rozdzielczości monitora w obiekcie zasobu po wykonaniu skanowania sprzętu
* Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM
* Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany
* Definiowanie statusów dla sprzętu (Nowy, Do kasacji, W serwisie, itd. )
* Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc. )
* Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe: Switch, Router, Access Point, Bridge, Modem, NAS, UPS, itd.)
* Automatyczne wykrywanie lokalnych drukarek (USB) na podstawie wyników skanowania sprzętu
* Automatyczne wykrywanie i tworzenie monitorów (producent, numer seryjny, rozdzielczość, odczyt firmy, działu, osoby odpowiedzialnej, głównego użytkownika)
* Automatyczne tworzenie zestawów: Komputer + Monitor
* Automatyczne utworzenie zestawów: Komputer + drukarka lokalna
* Automatyczne utworzenie zestawów: host+ maszyny wirtualne
* Automatyczne wykrywanie, czy komputer jest maszyną wirtualną
* Określanie informacji o wykorzystywanej wirtualizacji
* Podgląd zestawów, do których należy zasób
* Cykliczne wykonywanie skanowania sprzętu z różnymi ustawieniami
* Przypisywanie stałego atrybutu COA, który będzie uwzględniany na raportach wyposażenia i audytu
* Definiowanie szczegółowych informacji finansowych
* Definiowanie bazy dostawców sprzętu i oprogramowania
* Automatyczna aktualizacja adresów IP komputerów bez zainstalowanego agenta
* Określanie typu gwarancji dla zasobu

1. Raporty zasobów

* Raport dodanych załączników
* Automatyczne tworzenie historii zmian sprzętu
* Raport zbiorczy historii zmian w sprzęcie
* Ewidencja zdarzeń serwisowych
* Dodanie notatek\komentarzy dla zdefiniowanych obiektów zasobów
* Informacja na temat pojemności dysków twardych oraz wolnego miejsca
* Wydruk\dodanie jako załącznik protokołu przekazania\zwrotu\utylizacji sprzętu
* Wydruk\dodanie jako załącznik protokołu przekazania dla całego zestawu
* Definiowanie dedykowanych profili protokołów
* Zapisywanie protokołów podczas generowania jako załącznik do zasobu
* Wydruk\dodanie jako załącznik Karty informacyjnej dla elementu wyposażenia
* Wydruk lub zapisanie do pliku raportów ze szczegółami sprzętu
* Porównywarka wyników skanowania sprzętu
* Dzienniki zdarzeń systemu Windows
* Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu

1. Archiwum zasobów

* Przeniesienie utylizowanego wyposażenia do archiwum
* Automatyczne usunięcie informacji sieciowych oraz licencji agenta dla zasobu archiwizowanego
* Powiadomienia o kończącej się gwarancji\umowie serwisowej dla zasobu
* Zachowanie ostatniego skanu sprzętu podczas konserwacji bazy danych

1. Zarządzanie oprogramowaniem
2. Licencje

* Inwentaryzacja licencji
* Automatyczne tworzenie licencji na podstawie kluczy produktów
* Import licencji z pliku tekstowego
* Automatyczne generowanie historii zmian w licencji
* Określanie statusu licencji
* Utworzenie własnych atrybutów licencji
* Tworzenie notatek oraz załączników w dowolnym formacie do licencji
* Tworzenie zestawów licencji
* Relacja licencji z pracownikiem, firmą, działem, lokalizacją
* Zmiana typu licencji dla wybranej grupy
* Kompletna informacja na temat posiadanych licencji (typ, producent, program licencjonowania, czas ważności, informacje finansowe)
* Przypisywanie licencji do komputera
* Definiowanie wymaganych atrybutów legalności (faktura, nośnik, COA, etc.)
* Definiowanie ilości posiadanych licencji w rozbiciu na użytkowników oraz stanowiska
* Definiowanie licencji przeznaczonych do przyszłego zakupu
* Definiowanie kluczy seryjnych i przypisywanie do licencji
* Automatyczne usunięcie wiązania pomiędzy zasobem archiwizowanym a licencją

1. Skanowanie oprogramowania

* Skanowanie oprogramowania na podstawie harmonogramu oraz definicji skanera
* Automatyczna kontrola zmian w stanie zainstalowanego oprogramowania bez zlecania skanów
* Śledzenie zmian w stanie zainstalowanego oprogramowania
* Zdalny skan komputerów (bieżący lub okresowy)
* Zmiana priorytetu skanowania oprogramowania
* Skan komputerów niepodłączonych do sieci
* Przekazywanie konfiguracji wzorcowej dla skanera offline
* Identyfikacja zainstalowanych aplikacji na podstawie wzorców oprogramowania
* Prawidłowe rozpoznanie aplikacji nawet mimo zmiany jej nazwy
* Skan plików skompresowanych
* Skan oraz identyfikacja zawartości archiwów zapisanych w formatach: 7z, arj, bz2, bzip2, cab, gz, gzip, img, iso, jar, lha, lzh, lzma, msi, nrg, rar, tar, taz
* Wbudowane profile skanowania (np. profil wzorcowy)
* Definicja własnych ustawień skanowania
* Porównywanie wyników skanowania oprogramowania
* Wykrywanie plików multimedialnych
* Wykrywanie i inwentaryzacja plików dowolnego typu (np. multimedia, czcionki, grafika)
* Odczytywanie informacji o składnikach aplikacji, których programy instalacyjne nie są zgodne ze standardem MSI
* Identyfikacja SID użytkownika, dla którego zainstalowano oprogramowanie
* Bezpłatna, automatycznie aktualizowana baza wzorców aplikacji\pakietów\systemów operacyjnych
* Nadpisanie bazy wzorców najnowszą, oficjalną bazą producenta
* Definiowanie katalogów wykluczonych / uwzględnionych w skanowaniu z wykorzystaniem symboli wieloznacznych (\* , %)

1. Audyt legalności

* Rozliczanie pakietów aplikacji
* Rozliczanie systemów operacyjnych
* Rozliczanie licencji typu „Downgrade”, "Upgrade" oraz instalacji innego oprogramowania w ramach licencji
* Audyt oprogramowania rozliczany automatycznie - informacja o stanie posiadanych licencji i faktycznie zainstalowanych programach z uwzględnieniem wybranych zestawów licencji.
* Historia audytów (Wyniki audytów są przechowywane w bazie danych - można do nich wracać w dowolnej chwili, porównywać je i generować stosowne raporty)
* Wsparcie procesu Audytu przez zaimportowanie materiału zdjęciowego i jego obróbkę
* Gotowe metryki audytowanego komputera - załącznik do protokołu przekazania stanowiska komputerowego (sprzęt + oprogramowanie)
* Uwzględnianie w rozliczeniu oprogramowania liczby aktywacji zapisanej w szablonie licencji

1. Funkcje

* Mechanizm informujący o nowej bazie wzorców oprogramowania
* Definiowanie własnych wzorców oprogramowania
* Automatyczne tworzenie wzorców oprogramowania dla systemów operacyjnych
* Automatyczne dodawanie informacji o wydawcy oprogramowania dla nowych wzorców, tworzonych na podstawie wyników skanowania
* Wykrywanie kluczy/identyfikatorów programów
* W przypadku aktywacji systemu Windows z użyciem serwera KMS, klucza MAK (Multiple Activation Keys) lub VLK (Volume License Keys) odczytywane jest 5 ostatnich znaków klucza
* Odczytywanie informacji o częściowych kluczach pakietów Microsoft Office
* Drukowanie lub zapisywanie do pliku raportów ze szczegółami oprogramowania
* Zbiorcze raporty wyników skanowania oprogramowania - Pakiety, pliki, systemy operacyjne, kluczy zainstalowanych aplikacji
* Raport z informacjami o pakietach oprogramowania uwzględniający parametry: przybliżona wielkość, adres strony internetowej, lokalizacja pliku instalacyjnego, architektura aplikacji, itd.
* Raport z informacjami o systemach operacyjnych uwzględniający parametry: Data instalacji, Architektura systemu, Wersja kompilacji, itd.
* "Wielkie raporty" (Możliwość utworzenia zbiorczych raportów obejmujących np. wszystkie przeskanowane pliki)
* Zdalna instalacja dowolnego oprogramowania zgodnego ze standardem Windows Installer (\*.msi)
* Zdalne dezinstalacja oprogramowania
* Utworzenie harmonogramu dezinstalacji oprogramowania
* Generowanie skryptu deinstalacji aplikacji na podstawie otrzymanych wyników skanowania oprogramowania
* Raport stanu oprogramowania antywirusowego, anty-szpiegowskiego oraz zapory sieciowej
* Raport zainstalowanych aktualizacji systemu Windows

1. Kontrola wykorzystania sprzętu i oprogramowania
2. Pozyskiwanie informacji o pracownikach, zarządzanie widokami, funkcje ogólne

* Dane gromadzone dla konkretnych użytkowników (na bazie loginów) - jeden użytkownik może mieć przypisanych wiele loginów i pracować na różnych komputerach
* Grupowanie pracowników z podziałem na jednostki organizacyjne w firmie (np.względem działów)
* Określanie firmy do której należy pracownik
* Określanie przełożonego dla pracownika
* Prezentacja 'stanu pracownika' (obecny, nieobecny, nowy).
* Prezentacja 'statusu pracownika' (Zatrudniony, zwolniony, itd.)
* Przeniesienie rekordu pracownika do archiwum
* Funkcjonalności automatycznego generowania zmian rekordu pracownika – Historia pracownika
* Odczytywanie informacji o użytkownikach z Active Directory
* Pełna synchronizacja rekordów użytkowników (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory)
* Baza danych teleadresowych użytkowników z możliwością tworzenia raportów i zestawień
* Podgląd zdjęcia przypisanego do pracownika
* Przypisywanie do pracownika załączników (pliki)
* Przypisywanie do pracownika notatek.
* Ewidencja zdarzeń przypisanych do użytkowników
* Automatyczne tworzenie działów na podstawie informacji odczytanych z Active Directory

1. Raporty

* Analiza aktywności użytkowników
* Analiza zdarzeń sesji użytkownika (Logowanie, Wylogowanie, Zablokowanie, Odblokowanie, Nawiązanie połączenia RDP, Zakończenie połączenia RDP )
* Analiza przerw w pracy
* Analiza jakości pracy (liczba kliknięć myszą, liczba wpisanych znaków)
* Analiza wykorzystania poszczególnych aplikacji w czasie
* Analiza czasu działania aplikacji, na pierwszym planie oraz sumarycznie
* Kategoryzacja danych czasu pracy (czas pozytywny, neutralny oraz negatywny).
* Statystyki najczęściej wykorzystywanych aplikacji
* Statystyki wykorzystania komputerów przez poszczególnych użytkowników
* Statystyki aktywności pracownika i grup pracowników
* Generowanie raportów z monitoringu pracowników dla wybranego zakresu godzin
* Kontrola wydruków - historia zadań drukowania zainicjowanych przez poszczególnych użytkowników
* Informacje o drukowanych dokumentach (osoba, nazwa pliku, ilość stron, ilość kopii, cz-b/kolor, dpi)
* Monitoring wydruków na drukarkach sieciowych
* Informacja o operacjach na nośnikach zewnętrznych (CD/DVD, HDD, FDD, Pen Drive, etc.)
* Informacje o awariach, poczynaniach użytkowników: zakończonej aktualizacji, akcji podpięcia przenośnych dysków, włożenia płyt do napędów CD/DVD, śledzenie uruchomienia aplikacji przez użytkownika, monitoring informujący o małej ilości miejsca
* Raport zbiorczy historii zmian w rekordach pracowników

1. Funkcje

* Blokada niepożądanych aplikacji. Programy mogą być blokowane dla całej firmy lub tylko dla wybranych użytkowników.
* Autoryzacja nośników zewnętrznych
* Konfigurowanie praw dostępu do plików i katalogów zapisanych na nośnikach zewnętrznych
* Baza informacji o napędach zewnętrznych
* Blokada dostępu do napędów zewnętrznych (m.in. HDD, FDD, Pen Drive, etc.)
* Określanie praw dostępu w zależności od typu urządzenia, np. Pendrive, CD/ROM
* Komunikacja z użytkownikami (Skype, mail) bezpośrednio z zakładki Pracownicy
* Informacje o ostatnio zalogowanych osobach na stacjach klienckich
* Automatyczne tworzenie licencji – Dodawanie do licencji użytkowników, którzy są głównymi użytkownikami komputera, na którym wykryto licencje

1. Kontrola wykorzystania Internetu

* Blokada stron internetowych dla poszczególnych użytkowników, możliwość zastosowania filtrów, blokada WWW po zawartości (ContentType)
* Blokada stron internetowych dla protokołu http \ https (IE, Chrome, Firefox, Opera, Edge)
* Kategoryzacja stron internetowych
* Blokada dostępu do witryn zgodnie z harmonogramem
* Blokada trybu incognito w przeglądarce Google Chrome
* Raporty dotyczące aktywności użytkowników w Internecie oparte na loginach
* Dokładna analiza czasu przebywania na poszczególnych stronach lub domenach (z uwzględnieniem informacji o tytule strony i wersji przeglądarki )
* Monitoring stron internetowych dla protokołu http \ https (IE, Edge, Chrome, Firefox, Opera)
* Analiza liczby wejść na poszczególne strony lub domeny
* Analiza odwiedzanych domen i stron
* Raport informujący o plikach pobranych przez przeglądarki WWW
* Monitoring wysyłanych oraz pobieranych plików przez przeglądarki internetowe

1. Helpdesk

* Rejestracja i obsługa zgłoszeń
* Określanie relacji pomiędzy zgłoszeniami (np.. Kopia, Incydent nadrzędny)
* Kategoria zgłoszeń może posiadać swojego opiekuna, który może zarządzać każdym zgłoszeniem danej kategorii
* Komentarze zgłoszenia obsługujące HTML oraz osadzanie obrazów
* Opis zgłoszenia w formacie HTML
* Nawiązywanie połączeń zdalnych bezpośrednio z edytora incydent
* Tworzenie notatek dla zgłoszeń
* Zapisywanie wersji roboczej komentarza
* Archiwizacja zgłoszeń
* Monitoring czasu pracy nad incydentem (time tracking)
* Raport ewidencji czasu pracy nad zgłoszeniem
* Informacja o czasie reakcji do podjęcia zgłoszenia
* Dodanie prywatnego komentarza
* Znaki @ oraz # pozwalają na wspominanie użytkownika oraz wpisu bazy wiedzy w komentarzu zgłoszenia
* Dodanie załączników do incydentów, również do komentarza
* Określanie dodatkowych subskrybentów dla notyfikacji e-mail dotyczącej zmian w incydencie
* Określanie uprawnień do incydentów (Publiczne, Prywatne, dla określonych działów)
* Zarządzanie filtrami zdefiniowanymi dla listy zgłoszeń
* Obsługa nazwy DNS oraz adresów IP (IPv4, IPv6) dla zgłoszeń
* Wydruk historii zgłoszenia
* Widok kalendarza (Planowanie rozwiązania incydentów)
* Korelacja incydentu z elementem zasobów
* Raport zbiorczy historii zmian
* Tworzenie i planowanie zastępstw, osoba zastępująca otrzymuje na czas zastępstwa dostęp do obsługi zgłoszeń osoby zastępowanej
* Wyszukiwanie komentarzy przy użyciu funkcji globalnego wyszukiwania
* Czas reakcji oraz realizacji wyznaczany automatycznie na podstawie umów SLA
* Architektura drzewa dla kategorii zgłoszeń
* Tworzenie szablonów odpowiedzi
* Cykliczne raportowanie Listy incydentów
* Utworzenie własnych dodatkowych atrybutów dla zgłoszeń
* Notyfikacje e-mail o utworzeniu\zmianie\usunięciu incydentu
* Notyfikacje e-mail o zbliżających się terminach realizacji incydentu (Deadline)
* Automatyczny import wiadomości e-mail, jako zgłoszeń helpdesk
* Import zgłoszeń helpdesk ze skrzynek współdzielonych (shared mailbox)
* Obsługa wielu kont pocztowych (Import + notyfikację email)
* Tworzenie własnych trybów oraz priorytetów incydentów
* Personalizacja widoku raportu listy incydentów
* Profile zgłaszających w helpdesk
* Personalizacja kolorów statusów zgłoszeń
* Automatyczne przypisywanie zgłoszeń do użytkowników
* Monitoring pracy wykonywanej na komputerze
* Zdalny podgląd pulpitów wielu stacji ( Funkcja Company Online)
* Wywoływanie Windows Remote Desktop na danej stacji z poziomu aplikacji
* Wysyłanie wiadomości do użytkowników
* Zdalne uruchamianie komputera za pomocą funkcji Wake-On-Lan
* Przejęcie kontroli nad stacją roboczą
* Blokada klawiatury i myszki na stacji klienckiej w trakcie przejęcia kontroli pulpitu zdalnego
* Przesyłanie kombinacji klawiszy Ctrl + Alt + Delete w zdalnym pulpicie
* Przejęcie kontroli nad komputerem bez zalogowanego użytkownika
* Wysyłanie pytania o zgodę na zdalny dostęp lub wysyłania komunikatu z informacją o rozpoczęciu podglądu pulpitu
* Podgląd pulpitu zdalnego w osobnym oknie z opcją fullscreen
* Obsługa wielu monitorów dla podglądu pulpitu
* Wybór monitora, z którego ma być przekazywany obraz podglądu pulpitu
* Nawiązywanie połączenia pulpitu zdalnego z wieloma komputerami jednocześnie

1. Zarządzanie użytkownikami
2. Funkcje

* Raportowanie aktywności pracy
* Przeglądanie ostatnio zgłoszonych incydentów
* Powiązanie pracownika z licencją
* Dostęp webowy do statystyk monitoringu, zgłoszeń helpdesk oraz powiązanych z pracownikiem zasobów
* Cykliczne, automatyczne generowanie raportów
* Generowanie raportu obecności / nieobecności pracownika wraz z korelacją jego aktywności na komputerze
* Możliwość drukowania karty informacyjnej pracownika, zawierającej informacje kontaktowe, informacje o powiązanych zasobach, licencjach oraz dostępy nadane w module RODO
* Generator struktury organizacji na podstawie powiązań pracowników i ich przełożonych

1. Raportowanie cykliczne

* Raport historia sesji
* Raport Nośniki danych
* Raport Operacje na plikach
* Raport wydruków
* Raport użycia aplikacji
* Raport odwiedzonych stron WWW
* Raport czasu pracy przy komputerze
* Raport historii zasobów
* Raport informujący o nowych zasobach
* Raport informujący o nadchodzących terminach w zasobach
* Raport Zasoby zarchiwizowane
* Raport Informacje o autoryzowanych agentach
* Raport zainstalowanego oprogramowania
* Raport incydentów (Helpdesk)
* Raport czasu pracy nad zgłoszeniem

1. RODO

* Inwentaryzacja zbiorów danych, dostępów oraz powierzeń do zbiorów danych, dokumentów bezpieczeństwa, historii naruszeń bezpieczeństwa, szkoleń oraz wniosków o zapomnienie
* Wydruk raportów tabelarycznych: czynności przetwarzania, dostępów, powierzeń, listy dokumentów, statystyki zgłoszeń RODO, listę szkoleń, historii naruszeń bezpieczeństwa, wniosków o zapomnienie
* Wydruk wniosków o nadanie uprawnień, modyfikacji oraz anulowania upoważnienia
* Utworzenie zgłoszeń za pomocą przycisków szybkiej akcji
* Delegowanie zadań w helpdesk dla osób odpowiedzialnych za zbiory danych
* Archiwizacja zbiorów
* Definiowanie czynności przetwarzania
* Przypisywanie zbioru danych do czynności przetwarzania
* Przydzielanie dostępów do czynności przetwarzania
* Raporty zbiorcze: Czynności przetwarzania, Zbiory danych, zinwentaryzowanych dostępów, zinwentaryzowanych powierzeń, zinwentaryzowanych dokumentów, historii naruszeń bezpieczeństwa, wniosków o dostęp

1. Funkcjonalności ogólne

* Określanie praw dostępu do grup zasobów lub pracowników
* Aplikacja desktopowa służąca do zarządzania systemem może być zainstalowana na dowolnej liczbie komputerów ("Licencja pływająca")
* Dodatkowa aplikacja webowa umożliwiająca dostęp do systemu i zarządzanie systemem
* Praca w oparciu o silniki baz danych: MS SQL lub PostgreSQL
* Swobodna migracja danych pomiędzy MS SQL i PostgreSQL
* Zdalna instalacja i dezinstalacja agentów na stacjach roboczych
* Odczytywanie struktury organizacji z Active Directory
* Mechanizm automatycznego utworzenia komputera na podstawie danych przesłanych przez agenta
* Mechanizm automatycznego utworzenia pracownika na podstawie danych przesłanych przez agenta
* Automatycznie dodane komputery\pracownicy są powiązane z odpowiednią grupą zgodną z OU w Active Directory
* Definiowanie nieograniczonej liczby użytkowników systemu
* Określanie ról dla kont systemu: Administratorzy, Menadżerowie, Zarządcy
* Indywidualny login i hasło dla poszczególnych użytkowników
* Automatyczne logowanie do systemu
* Zarządzanie uprawnieniami użytkowników - możliwość ograniczenia dostępu do poszczególnych funkcji programu
* Zabezpieczenie Agentów przed nieautoryzowanym wyłączeniem lub usunięciem
* Eksport danych do plików zewnętrznych (Excel, html, CSV, PDF, TXT, MHT, RTF, BMP)
* Zgodny z pracą w sieciach WLAN
* Podgląd aktualnych zadań serwera
* Centrum informacji - przekrojowy raport na temat zdarzeń oraz statusu monitorowanych komputerów i użytkowników
* Wielopoziomowe drzewo lokalizacji
* Wyszukiwanie danych w tabelach raportów
* Dowolne definiowania grup sprzętu i użytkowników
* Utworzenie dowolnych raportów ad-hoc - sortowanie kolumn grupowanie, ukrywanie/odkrywanie kolumn, zaawansowane filtrowanie danych w oparciu o funkcje logiczne
* Definiowanie i zapamiętywanie własnych widoków
* Eksport danych bezpośrednio do MS Excel
* Obsługa protokołu SSL zapewniającego bezpieczną komunikację Master-Serwer oraz Agent-Server.
* Mechanizm zdalnego pobierania bieżących aktualizacji do programu
* Help kontekstowy wraz z podręcznikiem użytkownika w polskiej wersji językowej
* Dostęp do bazy wiedzy systemu
* Definiowanie ustawień pracy Agentów (optymalizacja dla dużej liczby komputerów)
* Dedykowane narzędzie, dostarczane z systemem, do wykonywania kopii bazy danych, niezależnie od wersji silnika bazy danych (MSSQL, PostgreSQL). Uruchomienie narzędzia backupu bazy w trybie wsadowym
* Automatyczna i manualna konserwacja bazy danych
* Manualna i automatyczna konserwacja bazy danych - usuwanie wyników skanowania oprogramowania
* Personalizacja pakietu instalacyjnego agenta
* Określanie polityki haseł dla systemu
* Globalne wyszukiwanie obiektów w systemie
* Utworzenie atrybutów jako lista/słownik
* Podgląd aktualnie zalogowanych użytkowników. Umożliwienie wylogowania wybranych użytkowników
* Definicja kalendarzy dni wolnych, uwzględnianych w module Helpdesk oraz Monitoring
  1. **Aktualizacja oprogramowania antywirusowego na stacje robocze i serwery wraz z konsolą do centralnej administracji**

|  |
| --- |
| Aktualizacja 320 szt. i rozszerzenie o kolejne 50 szt. licencji programu antywirusowego dla stacji roboczych i serwerów.  Aktualizacja posiadanego przez zamawiającego oprogramowania Eset Endpoint Protection Standard poprzez dostarczenie 320 licencji ww. oprogramowania i rozszerzenie o kolejne 50 szt. 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 (Security Management Centre). Subskrypcja aktualizacji bazy danych wirusów dla ww. licencji ma obowiązywać przez rok od 19 listopada 2021 r.  Zamawiający dopuszcza zastosowanie innego, równoważnego\* rozwiązania pod warunkiem, że spełnia ono minimalne parametry przedstawione w poniższej specyfikacji:  **Stacje Windows**  1. Pełne wsparcie dla systemu Windows 7, 8, 8.1 i 10.  2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.  3. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim.  4. 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**  Wsparcie dla systemów:   * Microsoft Windows Server 2008 (x86 and x64), 2008 R2, 2012, 2012 R2, 2016, * Microsoft Windows Storage Server 2008 R2 Essentials SP1, 2012, 2012 R2, * Microsoft Windows Small Business Server 2003 (x86), 2003 R2 (x86), 2008 (x64), 2011 (x64), * Microsoft Windows Server 2012 Essentials, 2012 R2 Essentials, * Microsoft MultiPoint Server 2010, 2011, * Windows MultiPoint Server 2012.  1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 3. Wbudowana technologia do ochrony przed rootkitami i exploitami. 4. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 5. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 6. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 7. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. 8. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego. 9. Możliwość skanowania dysków sieciowych i dysków przenośnych. 10. Skanowanie plików spakowanych i skompresowanych. 11. 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. 12. Aplikacja powinna wspierać mechanizm klastrowania. 13. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 14. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. 15. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 16. 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. 17. 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. 18. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 19. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 20. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. 21. Dodanie automatycznych wyłączeń nie wymaga restartu serwera. 22. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. 23. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. 24. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione. 25. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego. 26. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). 27. 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. 28. 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. 29. 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. 30. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 31. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e‑mail. 32. 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. 33. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo. 34. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC. 35. 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. 36. 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. 37. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 38. 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. 39. 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. 40. 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. 41. 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). 42. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 43. Aplikacja musi wspierać skanowanie magazynu Hyper-V 44. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów 45. 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). 46. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 47. 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. |

**Część 2**

**a) laptop wraz z oprogramowaniem systemowym i wyposażeniem – 38 szt.,**

**b) oprogramowanie Microsoft Office Home and Business 2019 PL lub równoważne – 38 szt.**

|  |  |
| --- | --- |
|  | **Opis wymaganych parametrów technicznych** |
| **1** | **2** |
| 1.1 | Typ: laptop |
| 1.2 | Wydajność: laptop osiągający ogólny wynik 1000 pkt w teście Bapco Sysmark 2018  oraz wynik testu składowego Overall Rating - Office Productivity min. 910 punktów  Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta. |
| 1.3 | Pamięć: nie mniej niż 8 GB, gniazda na pamięć (ogółem/wolne) 2/1, możliwość rozszerzenia do 32GB pamięci. |
| 1.4 | Dysk twardy SSD min. 512 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 |
| 1.12 | 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. |
| 1.13 | Wbudowany napęd DVD-RW |
| 1.14 | Bateria: 3-komorowa, min. 3500 mAh, Li-Ion |
| 1.15 | Zasilacz: Tak |
| 1.16 | Waga: do 2 kg (z baterią) |
| 1.17 | 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 |
| 1.18 | 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 |
| 1.19 | Dołączone wyposażenie do każdego laptopa: |
| Mysz optyczna, rolka, standard – USB |
| Torba w ciemnym kolorze |
| 1.20 | Gwarancja – min.24 miesiące |

**Część 3**

1. **system centralnego zarządzania zdalnym dostępem VPN z licencją na 50 stacji roboczych**

W ramach postepowania wymagane jest dostarczenie rozwiązania do zarządzania, konfiguracji dostępu VPN dla stacji roboczych wraz z mechanizmami centralnego zarządzania.

Dostarczone rozwiązanie musi zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się, aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji.

Parametry systemu zarządzania dostępem VPN dla stacji roboczych:

1. Elementy systemu zarządzania z dostępem dla stacji roboczych muszę zawierać następujące funkcje i mechanizmy:
   1. Kategoryzacja URL
      1. URL filtering w oparciu o kategorie stron z opcją definiowania wyjątków.
      2. Możliwość integracji z wtyczką do przeglądarki internetowej, celem analizy kategorii WWW dla ruchu SSL/HTTPS
      3. System musi umożliwiać filtrowanie
   2. Analiza podatności
      1. Mechanizmy analizy podatności na stacji roboczej - pozwalające wykryć zagrożenia w systemie operacyjnym oraz zainstalowanych aplikacjach.
      2. Mechanizmy pozwalające na wymuszenie aktualizacji systemu lub popularnych aplikacji
   3. Dostęp VPN
      1. Mechanizmy szyfrowanych połączeń typu IPSec VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
      2. Mechanizmy szyfrowanych połączeń typu SSL VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu.
      3. Rozwiązanie musi umożliwiać realizowanie funkcjonalności split tunneling w oparciu o aplikacje, przykładowo musi istnieć możliwość wykluczenia aplikacji wymagających dużej ilości pasma np.: Microsoft Office 365, Microsoft Teams, Skype, GoToMeeting,Zoom, WebEx, YouTube
      4. Rozwiązanie musi umożliwiać realizowanie funkcjonalności split tunneling w oparciu o domeny (FQDN)
      5. Możliwość zastosowania certyfikatów cyfrowych w procesie uwierzytelnienia przy realizacji szyfrowanych połączeń.
      6. Mechanizmy uwierzytelniania dwuskładnikowego.
      7. System musi umożliwiać zastosowanie protokołu SAML dla SSL VPN
2. Funkcjonalność kontroli i blokowania urządzeń USB
3. System musi umożliwiać określanie czy dana stacja znajduje się w wewnętrznej sieci chronionej, czy poza nią, na podstawie reguł budowanych w oparciu cechy :
   1. Parametrów DHCP
   2. Serwerów DNS
   3. Połączenia ze stacją zarządzającą
   4. Adresacją sieci
   5. Bramą domyślną (Default Gateway) (adres IP lub adres MAC)
   6. Publiczny adres IP
   7. Tunel VPN
   8. Dostępny IP za pomocą PING
   9. Typ połączenia (Ethernet lub WiFI)
4. Reguły określające czy stacja należy do sieci zaufanej muszą być budowane w oparciu o różne kombinacje powyższych parametrów
5. Reguły muszą pozwalać na przydzielenie różnych profili bezpieczeństwa zależnie od określenia przynależności do sieci zaufanej
6. Centralne logowanie i raportowanie
   1. System musi umożliwiać wysyłanie logów o ze stacji roboczych do centralnego systemu logowania i raportowania
7. Centralne zarządzanie
   1. System musi umożliwiać centralne zarządzania stacjami roboczymi
8. Poszczególne mechanizmy muszą być dostępne dla następujących wersji systemów operacyjnych Windows oraz Mac OS: Microsoft Windows 10 (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit), Windows 8 (32-bit, 64-bit), Windows Server 2016, Windows Server 2008 R2, Windows Server 2012, 2012 R2.

# Parametry systemu centralnego zarządzania.

1. Dostarczony system centralnego zarządzania aplikacjami klienckimi musi zapewniać wszystkie wymienione poniżej funkcje. Wymaga się aby elementy wchodzące w skład systemu były zrealizowane w postaci komercyjnych platform wirtualnych lub aplikacji instalowanych na systemach operacyjnych: Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2.
2. System powinien umożliwiać automatyczną aktualizację oprogramowania na urządzeniach końcowych oraz musi zapewniać mechanizmy integracji z sieciowymi systemami bezpieczeństwa, w tym co najmniej: Firewall.
3. Ponadto wymagane jest aby system zapewniał:
   1. Integrację z systemami zarządzania tożsamością użytkowników – co najmniej AD.
   2. Definiowanie różnych profilów (wersji konfiguracji) dla różnych grup użytkowników czerpanych z AD lub definiowanych lokalnie.
   3. Zautomatyzowany proces zarządzania aplikacja kliencką.
   4. Przygotowywanie paczek instalacyjnych przynajmniej dla systemu Windows 32/64 bit, w których administrator może określić komponenty dla instalatora dla stacji roboczych takich jak: filtrowanie URL, analiza podatności, agent tożsamości współpracujący z centralnym serwerem uwierzytelniania (SSO)
   5. Możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym.
   6. Panel, w którym wyświetlane są wyniki analizy podatności na stacjach roboczych.
   7. Panel w którym wyświetlane są informacje o podłączonych i zarządzanych stacjach roboczych:
      1. System musi umożliwiać wyświetlanie w konsoli zarządzania informacji o stacjach roboczych, które mogą służyć do diagnozy problemów oraz stanu stacji min:
         * Typ połączenia (Ethernet/Wifi)
         * Adres IP
         * Adres IP domyślnej bramy
         * Adres MAC
         * Adres MAC bramy sieciowej
         * Nazwa sieci WiFi (SSID)
         * Model sprzętu
         * Producent sprzętu
         * Informacje o procesorze
         * Informacje o pamięci RAM
         * Numer seryjny
         * Informacje o dysku twardym (rozmiar)
4. Możliwość wymuszenia aktualizowania systemu i aplikacji z racji wykrytych podatności na stacjach roboczych.
5. Automatyczne wykrywanie stacji klienckich w grupach roboczych.
6. Logowanie zdarzeń z aplikacji klienckich, możliwość ich przeglądania z funkcja filtrów oraz możliwością pobierania logów przez administratora.
7. Generowanie alarmów: związanych z zarządzeniem aplikacją kliencką, w przypadku wykrycia ważnych podatności na stacjach.
8. Definiowanie grup administratorów lokalnie oraz w oparciu o AD z opcja przypisywania uprawnień do elementów panelu konfiguracyjnego.
9. Zarządzenie certyfikatami na potrzeby połączeń IPSec VPN oraz SSL VPN.
10. Automatyczne wykrywanie aplikacji zainstalowanych na stacjach klienckich z możliwością filtrowania przynajmniej po producencie i nazwie aplikacji.
11. Możliwość przeniesienia użytkownika do kwarantanny i personalizację komunikatu, który wyświetli się użytkownikowi.
12. Możliwość wymuszenia przeskanowania stacji klienckiej za pomocą antywirusa i skanera podatności na żądanie jak i cyklicznie,
13. Możliwość skonfigurowania weryfikacji zgodności (compliance) w celu sprawdzenia czy na stacji końcowej jest aktualna baza sygnatur dla AV, czy jest odpowiednia wersja systemu operacyjnego, czy jest uruchomiony odpowiedni proces.
14. Administrator musi mieć możliwość wykonywania backupu i odtwarzania bazy danych, w oparciu o którą działają elementy system.
15. Centralny system zarządzania musi zapewniać możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora lub w ramach postępowania koniecznym jest dostarczenie odpowiednio zabezpieczonego portalu, za pośrednictwem którego administrator będzie mógł dystrybuować paczki instalacyjne.

W ramach postępowania wraz z konsolą centralnego zarządzania muszą zostać dostarczone niezbędne licencje upoważniające do:

1. Zainstalowania i centralnego zarządzania minimum 50 licencji aplikacjami klienckimi na stacjach roboczych.
2. Dla wskazanej powyżej ilości stacji roboczych licencje powinny obejmować funkcjonalności:
   1. Filtrowanie adresów URL
   2. Możliwość zarządzania stacjami roboczymi i profilami SSL i IPSec VPN
   3. Możliwość wykonywania analizy podatności systemów operacyjnych i zainstalowanych aplikacji
   4. Centralne zarządzanie
   5. Centralne logowanie i raportowanie
   6. Kontrolę urządzeń USB
   7. Wsparcie dla uwierzytelniania wieloskładnikowego
   8. Komponentu/agenta pozwalającego na wysyłanie informacji o aktualnie zalogowanym użytkowniku w ramach infrastruktury AD, pozwalającej na budowę transparentnego mechanizmu Single Sign On.
3. System musi być objęty wsparciem technicznym przez okres minimum 12 miesięcy, upoważniającym do aktualizacji oprogramowania.
4. System musi być dostarczony z licencją na konsolę zarządzającą oraz 50 stacji roboczych na okres minimum 12 miesięcy.
5. **Dostawa przełączników sieciowych – 12 szt.**
6. Minimum 48 portów 10/100/1000BaseT ze wsparciem dla standardu PoE+ (802.3at)
7. Minimum 4 porty 1/10GbE SFP+, niezależne od wymaganych portów 10/100/1000BaseT
8. Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT
9. Wydajność przełączania co najmniej 176 Gbps oraz przepustowość 112 Mpps dla pakietów 64 bajtowych
10. Obsługa 4094 tagów IEEE 802.1Q oraz minimum 512 jednoczesnych sieci VLAN Automatyczne wykrywanie punktów bezprzewodowych podłączonych do przełącznika automatyczne konfigurowanie portów, do których są one podłączone (minimum sieć VLAN, CoS, budżet mocy PoE, priorytet PoE)
11. Funkcja automatycznej aprowizacji i konfiguracji przełącznika przy jego pierwszym podłączeniu do sieci bez konieczności wykonywania wstępnej, ręcznej konfiguracji Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
12. Budżet mocy PoE nie może być mniejszy niż 360W
13. Bufor pakietów nie mniejszy niż 12MB
14. Minimum 2GB pamięci Flash
15. Dostęp do urządzenia przez konsolę szeregową (linia komend umożliwiająca pełne zarządzanie przełącznikiem), HTTPS, SSHv2 i SNMPv3

Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)

Obsługa Secure FTP

Obsługa 802.3ad Link Aggregation Protocol (LACP)

Obsługa Simple Network Time Protocol (SNTP) v4

1. Wielkość tablicy adresów MAC: minimum 16000
2. Obsługa LLDP i LLDP-MED
3. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting
4. Funkcja autoryzacji użytkowników zgodna z 802.1x
5. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+,
6. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
7. Obsługa list kontroli dostępu (ACL)
8. Obsługa protokołu TR-069
9. Obudowa wieżowa 1U umożliwiająca instalację w szafie 19" o głębokości nie większej niż 35 cm.
10. Maksymalny pobór mocy (bez PoE) nie większy niż 60W
11. Minimalny zakres pracy od 0°C do 45°C
12. 10 letnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wymagane jest zapewnienie technicznego producenta (niezależnego od zgłaszania usterek) wsparcia telefonicznego w trybie 8x5 przez okres co najmniej 10 lat. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis.
13. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.

**c) Usługa wsparcia technicznego systemu do backupu Veeam Backup Essentials Enterprise**:

1. wsparcie dla posiadanego rozwiązania „Veeam Backup Essentials Enterprise. Public Sector. 2 socket pack” w wersji Basic,
2. praca serwisanta aż do rozwiązania problemu,
3. czas przystępowania do diagnozowania nie dłuższy niż 5 godz.,
4. możliwość telefonicznego zgłaszania awarii w trybie 9 godzin na dobę od 8:00 do 17:00 dla serwisu następny dzień roboczy NBD,
5. bezpośredni, rejestrowany dostęp do centrum pomocy technicznej producenta przez 24 godziny na dobę, umożliwiający bezpośrednie, samodzielne otwieranie przez zamawiającego zgłoszeń serwisowych w centrum pomocy technicznej producenta bez limitu na ilość zapytań,
6. wymiana dysku obejmuje opcję „zachowaj swój dysk” (w przypadku awarii nośnika danych – dysku twardego, serwis producenta wymienia nośnik bez konieczności zwrotu uszkodzonego nośnika) przez cały okres wsparcia,
7. dostęp do najnowszego oprogramowania sprzętowego urządzeń, możliwość pobrania najnowszego oprogramowania ze strony producenta,
8. naprawa uszkodzonego urządzenia w miejscu instalacji (on-site),
9. okres wsparcia: 12 miesięcy.