Numer sprawy: OZP.261.13.2023.ŁF

Załącznik Nr 7 do SWZ

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

1. Przedmiotem zamówienia dostawa sprzętu niezbędnego do wdrożenia systemu do elektronicznego zarządzania dokumentacją (EZD), serwera NAS oraz dysków do serwera NAS - backup przeznaczony do systemu elektronicznego zarządzania dokumentacją (EZD), sprzętu komputerowego, urządzenia wielofunkcyjnego oraz sprzętu elektronicznego wraz z akcesoriami.
2. Zakres przedmiotowy zamówienia z podziałem na 3 części:

|  |  |  |  |
| --- | --- | --- | --- |
| **CZĘŚĆ I** - **DOSTAWA SPRZĘTU KOMPUTEROWEGO NIEZBĘDNEGO DO WDROŻENIA SYSTEMU DO ELEKTRONICZNEGO ZARZĄDZANIA DOKUMENTACJĄ (EZD)** | | | |
| 1. **SERWER – 1 SZT.** | | | |
|  | **PARAMETR** | **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE** | |
| **1.** | **Obudowa** | Obudowa Rack o wysokości max. 2U umożliwiającą instalację min. 8 dysków 3,5” z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. | |
| **2.** | **Płyta główna** | Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. | |
| **3.** | **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. | |
| **4.** | **Procesor** | Zainstalowane dwa procesory min. ośmio-rdzeniowe klasy x86 do pracy z zaoferowanym serwerem. Zaoferowany serwer w konfiguracji dwuprocesorowej musi osiągać wyniku min. 143 punkty w teście SPECrate2017\_int\_base dostępny na stronie www.spec.org. W celu weryfikacji tego parametru wynik testu załączyć do oferty. | |
| **5.** | **RAM** | Min. 128GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM. | |
| **6.** | **Zabezpieczenia pamięci RAM** | Advanced ECC, Memory Health Check, Memory Page Retire. | |
| **7.** | **Gniazda PCIe** | Minimum 1 sloty PCIe x16 generacji min. 3 oraz 1 slot PCIe x4 generacji min. 3. | |
| **8.** | **Interfejsy sieciowe** | * dwa interfejsy 1Gb Ethernet RJ45; * dwa interfejsy sieciowe 10Gb Ethernet w standardzie SFP+, dla każdego portu SFP+ należy dostarczyć kabel direct-attach o długości min. 3 metrów; | |
| **9.** | **Dyski twarde** | Zainstalowane dyski:   * 2 x 960 GB SSD SATA RI 6Gbps 512 2.5in Hot-plug; * 6 x 8TB 7200 RPM NLSAS 12Gbps 3.5in Hot-plug;   Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmiejszenia ilości wnęk na dyski twarde. | |
| **10.** | **Kontroler RAID** | Sprzętowy kontroler dyskowy PCI-E z pojemnością cache 8GB, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60. | |
| **11.** | **Wbudowane porty** | Min. port USB 2.0 oraz port USB 3.0, port VGA. | |
| **12.** | **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900. | |
| **13.** | **Wentylatory** | Redundantne. | |
|  | **Zasilacze** | Min. dwa zasilacze Hot-Plug maksymalnie 800W. | |
| **14.** | **Bezpieczeństwo** | Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.  Możliwość wyłączenia w BIOS funkcji przycisku zasilania.  BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła .  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.  Moduł TPM 2.0 v3  Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera.  Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. | |
| **15.** | **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; * możliwość podmontowania zdalnych wirtualnych napędów; * wirtualną konsolę z dostępem do myszy, klawiatury; * wsparcie dla IPv6; * wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH; * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz; * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; * integracja z Active Directory; * możliwość obsługi przez ośmiu administratorów jednocześnie; * wsparcie dla automatycznej rejestracji DNS; * wsparcie dla LLDP; * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej; * możliwość podłączenia lokalnego poprzez złącze RS-232; * możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy; * Monitorowanie zużycia dysków SSD; * możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi; * automatyczne zgłaszanie alertów do centrum serwisowego producenta; * automatyczne update firmware dla wszystkich komponentów serwera; * możliwość przywrócenia poprzednich wersji firmware; * możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON; * możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych; * automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram; * możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera;   Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI. | |
| **16.** | **System Operacyjny** | Microsoft Windows Server 2022 Standard lub równoważny.  Licencja bezterminowa zgodna z liczbą fizycznych rdzeni procesorów zainstalowanych w oferowanym serwerze  Opis równoważności dla Systemu Operacyjnego:  Cechy równoważnego oprogramowania typu Microsoft Windows Server 2022 Standard Edition:   1. Zamawiający dopuszcza zastosowanie oprogramowania równoważnego, poprzez które należy rozumieć oferowane oprogramowanie o parametrach nie gorszych od opisanych jako wymagane, umożliwiające wykorzystanie urządzeń, w takim samym zakresie i stopniu skomplikowania, co oprogramowanie określone w opisie przedmiotu zamówienia. 2. Oferowany system operacyjny musi posiadać następujące cechy, funkcje i minimalne parametry:    1. współpraca z procesorami o architekturze x86-64;    2. instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym;    3. obsługa dostępu wielościeżkowego do zasobów LAN poprzez kontrolery Gigabit Ethernet, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu;    4. zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie minimum Microsoft Windows Server 2019;    5. licencja musi uprawniać do uruchamiania wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji;    6. możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci;    7. automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego;    8. wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji;    9. możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET;    10. możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych;    11. graficzny interfejs użytkownika. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe;    12. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play);    13. możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu;    14. dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management);    15. możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  * podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC; * usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach; * pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe; * zdalna dystrybucja oprogramowania na stacje robocze; * praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej; * PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:   - Dystrybucję certyfikatów poprzez http;  - Konsolidację CA dla wielu lasów domeny;  - Automatyczne rejestrowania certyfikatów pomiędzy rożnymi lasami domen;  - Szyfrowanie plików i folderów;  - Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec);  - Serwis udostępniania stron WWW;  - Wsparcie dla protokołu IP w wersji 6 (IPv6);  - Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows;   * 1. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet;   2. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath);   3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty;   4. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF;   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. | |
| **17.** | **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-14001, ISO 50001.  Serwer musi posiadać deklaracja CE.  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2019 x64, Microsoft Windows 2022. | |
| **18.** | **Normy Środowiskowe** | Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku. | |
| **19.** | **Warunki gwarancji** | 36 miesięcy gwarancji producenta z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu. | |
| **20.** | **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. | |
| **21.** | **Warunki dodatkowe** | Zamawiający wymaga instalacji fizycznej serwera w serwerowni Zamawiającego oraz konfiguracji, instalacji na nim posiadanego przez Zamawiającego oprogramowania i przeszkolenie pracownika Zamawiającego. | |
| 1. **DOSTAWA LICENCJI DOSTĘPOWYCH CAL NA UŻYTKOWNIKA – 60 SZT.** | | | |
|  | **Charakterystyka** | Licencje dostępowe muszą umożliwiać dostęp każdemu użytkownikowi z dowolnego urządzenia do posiadanego przez Zamawiającego systemu serwerowego Windows Server 2022 Standard. | |
| 1. **DOSTAWA LICENCJI TERMINALOWYCH RDS NA UŻYTKOWNIKA – 10 SZT.** | | | |
|  | **Charakterystyka** | Licencje muszą umożliwiać korzystanie z serwera terminalowego opartego o usługę Microsoft Windows Server do publikacji aplikacji i zdalnego dostępu do zasobów realizowanego z sieci LAN/WAN. | |
| 1. **DOSTAWA LICENCJI SERWEROWEGO SYSTEMU BAZODANOWEGO – 1 SZT.** | | | |
|  | **Charakterystyka** | Licencja bezterminowa, Zamawiający dopuszcza możliwość dostawy licencji oprogramowania równoważnego, o parametrach nie gorszych niż wskazane, o ile będzie to oprogramowanie w pełni zgodne i kompatybilne z używanymi przez Zamawiającego aplikacjami.  Wymagania minimalne:.   * oprogramowanie silnika baz danych przeznaczone do instalacji w ramach lokalnej infrastruktury sprzętowej i programowej posiadanej przez Zamawiającego; * ilość oferowanych licencji oprogramowania silnika baz danych musi zapewnić wykorzystanie mocy obliczeniowej min. 8 rdzeni procesora oraz min. 32GB pamięci RAM; * ilość oferowanych licencji oprogramowania silnika baz danych musi umożliwiać pełne wykorzystanie silnika dla min. 3 użytkowników z nieograniczonej puli stanowisk dostępowych; * zarządzanie silnikiem baz danych dostępne będzie z poziomu narzędzia graficznego (aplikacja typu desktop lub aplikacja obsługiwana w przeglądarce WWW). Wszystkie funkcje zarządzania muszą być dostępne lokalnie bez wymaganego dostępu do sieci Internet. Narzędzie graficzne do zarządzania silnikiem musi zapewniać możliwość zarządzania i konfiguracji wszystkich usług implementowanych przez silnik baz danych; * dostępna funkcja profilowania silnika baz danych, rejestrująca określone wg filtra zapytania spływające do silnika baz danych w czasie rzeczywistym w formie dziennika zdarzeń, której zadaniem będzie identyfikacja ewentualnych problemów lub błędów w działaniu aplikacji; * zarządzanie silnikiem baz danych dostępne będzie z poziomu narzędzia linii poleceń umożliwiające automatyzację czynności administracyjnych, min.: * wykonywanie zadań kopii zapasowych; * zarządzanie kontami użytkowników; * zarządzanie uprawnieniami użytkowników; * zarządzanie pracą silnika baz danych (min. akcje uruchomienia i zatrzymania pracy silnika); * Wykonywanie zapisanych skryptów poleceń SQL z obsługą przekierowywania wyjścia na standardowe wyjście konsoli lub do pliku; * obsługa aktualizacji automatycznych dla silnika musi umożliwiać automatyczne ściąganie i instalację poprawek bezpieczeństwa producenta oprogramowania dla minimalizacji zagrożeń powodowanych przez wykryte luki w zabezpieczeniach oprogramowania silnika; * silnik baz danych musi posiadać mechanizm pozwalający na duplikację określonych baz danych między dwiema instancjami, zapewniający replikację danych w czasie rzeczywistym; * silnik baz danych musi obsługiwać mechanizm kompresji kopii zapasowych w trakcie ich tworzenia; * obsługa automatycznego szyfrowania kopii zapasowych baz danych (w trakcie wykonywania) przy użyciu min. funkcji kryptograficznej AES-256 z użyciem klucza asymetrycznego. Możliwość szyfrowania kopii zapasowych baz danych niezaszyfrowanych; * wsparcie dla zastosowanych w MIK reguł bezpieczeństwa, min. zastosowanie mechanizmu weryfikacji dostatecznego poziomu długości i komplikacji haseł użytkowników, możliwość zintegrowania uwierzytelniania użytkowników z Active Directory; * automatyczne rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym o następujących cechach: * zredukowany do minimum negatywny wpływ logowania na wydajność silnika baz danych; * możliwość selektywnego wybierania rejestrowanych zdarzeń takich jak: monitorowanie stanu obciążenia silnika, operacje odczytu i zapisu danych na dysku, przekroczenie czasu wykonywania operacji, aktywność użytkownika; * możliwość definiowania nowych typów danych przechowywania z obsługą danych hierarchicznych. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Wykonawcę języku programowania; * obsługa danych w formacie XML w zakresie umożliwiającym składowanie i obróbkę danych w postaci struktur XML. Silnik musi zapewniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli oraz zapewnić mechanizm do walidacji struktur XML wykorzystując szablony XSD. Ponadto silnik musi udostępniać język zapytań zgodny ze standardem XQuery do obsługi struktur XML; * obsługa tworzenia funkcji i procedur w innych językach programowania z możliwością ich uruchomienia z poziomu zapytań SQL lub wyzwalaczy SQL Trigger;   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.  Licencja odpowiednio dobrana do zaoferowanego w pkt. 1 serwera | |
| 1. **LICENCJA DOSTĘPOWA SQL CAL NA UŻYTKOWNIKA DOBRANA ODPOWIEDNIO DO ZAOFEROWANEGO SYSTEMU BAZODANOWEGO – 60 SZT.** | | | |
|  | **Charakterystyka** | Licencje dostępowe muszą umożliwiać dostęp każdemu użytkownikowi z dowolnego urządzenia do posiadanego przez Zamawiającego oprogramowania bazodanowego Microsoft SQL Server 2022 Standard. | |
| 1. **SKANER DOKUMENTÓW – 2 SZT.** | | | |
|  | **PARAMETR** | **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE** | |
| **1.** | **Typ skanera** | Skaner z automatycznym podajnikiem dokumentów ADF  oferowany skaner musi poprawnie współpracować z systemem elektronicznego zarządzania dokumentami (EZD PUW). | |
| **2.** | **Tryb skanowania** | Skanowanie dwustronne jednoprzebiegowe (duplex); kolor/skala szarości/monochromatyczny. | |
| **3.** | **Przeznaczenie urządzenia** | Skanowanie dokumentów o różnych formatach i gramaturach bez konieczności ich wcześniejszej segregacji. | |
| **4.** | **Format skanowanych dokumentów** | A4, A5,A6,A7,B5,B6,B7 i mniejsze. | |
| **5.** | **Ilość układów optycznych** | 2 - możliwość skanowania w trybie duplex z ADF. | |
| **6.** | **Element światłoczuły dla ADF** | CIS. | |
| **7.** | **Prędkość skanowania dla 300 DPI tryb cz&b, skala szarości, kolor** | Minimum 60 arkuszy/min, minimum 120 obrazów/min. | |
| **8.** | **Rozdzielczość optyczna** | 600 DPI. | |
| **9.** | **Rozdzielczość wyjściowa** | 100-1200 DPI. | |
| **10.** | **Panel kontrolny** | Kolorowy LCD, z polskim interfejsem użytkownika o wielkości co najmniej 3,5 cala z możliwością predefiniowania profili skanowania, ich indywidualnego opisu i uruchamiania z poziomu skanera. | |
| **11.** | **Automatyczny podajnik dokumentów** | 80 arkuszy A4 o gramaturze 80g/m2. | |
| **12.** | **Tryb skanowania kopert** | Opcjonalnie A3 lub A4. | |
| **13.** | **Poprawa jakości skanowanych dokumentów dla Twain i ISIS** | Likwidacja przekosu, automatyczne rozpoznawanie wielkości i rozmiaru dokumentu, usuwanie kolorów; skanowanie dwustrumieniowe kolor i czarno-biały za jednym przebiegiem; interaktywna regulacja koloru, regulacja jasności i kontrastu, automatyczna rotacja dokumentu, automatyczne wykrywanie koloru, inteligentne wygładzanie koloru tła, inteligentne wypełnienie krawędzi obrazu, scalanie obrazów, wykrywanie pustych stron na podstawie procentowej zawartości oraz rozmiarze pliku, filtrowanie smug, filtr ostrości, fizyczne układanie dokumentów do krawędzi (likwidacja przekosu). | |
| **14.** | **Format plik wyjściowego** | tiff, jpg, bmp, pdf, pdf przeszukiwalny do j. polskiego, doc,xls oraz rtf do j. polskiego. | |
| **15.** | **Format pliku indeksowego** | Możliwość generowania pliku xml lub csv - zawierającego informację na temat liczby zeskanowanych stron, nazwy pliku oraz wartości odczytanego kodu kreskowego np.: Interleaved 2 of 5, Code 3 of 9, Code 128, Codabar, UPC-A, UPC-E, EAN-13, EAN-8, PDF417, QR code. | |
| **16.** | **Wsparcie dla sterowników** | Możliwość generowania pliku xml lub csv - zawierającego informację na temat liczby zeskanowanych stron, nazwy pliku oraz wartości odczytanego kodu kreskowego np.: Interleaved 2 of 5, Code 3 of 9, Code 128, Codabar, UPC-A, UPC-E, EAN-13, EAN-8, PDF417, QR code. | |
| **17.** | **Interfejs komunikacyjny z PC** | USB 3.1 lub szybszy, LAN wbudowany w urządzenie, WIFI. | |
| **18.** | **Obciążenie dzienne** | Minimum 8 000 skanów. | |
| **19.** | **Maksymalna wspierana przez skaner długość dokumentu** | 3000 mm. | |
| **20.** | **Zakres gramatury skanowanych dokumentów dla ADF** | Od 27g/m2 do 433g/m2. | |
| **21.** | **Ochrona dokumentów przed zgnieceniem za pomocą czujnika akustycznego** | Tak - z regulacją poziomu czułości w sterowniku skanera. | |
| **22.** | **Czujnik podwójnych pobrań dokumentów** | Tak. | |
| **23.** | **Wsparcie producenta dla skanowania kart** | Tak. | |
| **24.** | **Aplikacja do odczytu kodów kreskowych** | Tak. | |
| **25.** | **Wspierane systemy operacyjne dla sterowników TWAIN oraz ISIS** | Windows 7 SP1 (wersja 32-bitowa i 64-bitowa), Windows 8 (wersja 32-bitowa i 64-bitowa), Windows 8.1 (wersja 32-bitowa i 64-bitowa), Windows 10 (wersja 32-bitowa i 64-bitowa), Windows Server 2012 x64, Windows Server 2016 x64, Linux. | |
| **26.** | **Zarządzanie i monitoring** | Skaner musi współpracować z aplikacją do zdalnej aktualizacji sterowników z poziomu serwera oraz umożliwiać zdalną konfiguracja profili skanowania z poziomu serwera, generowanie raportów dotyczących stanu zużycia skanera i części eksploatacyjnych, generowanie monitów dotyczących np. potrzeby przeprowadzenia konserwacji skanera. | |
| **27.** | **Gwarancja** | 36 miesięcy NBD. | |
| **28.** | **Waga** | Do 3,5kg. | |
| **29.** | **Pobór mocy** | Tryb pracy do 36W, do 5W w trybie uśpienia. | |
| **30.** | **Deklaracja zgodności** | Urządzenie musi posiadać oznakowanie CE. | |
| **31.** | **Ochrona środowiska** | Oferowany sprzęt musi spełniać wymogi specyfikacji technicznej Energy Star i posiadać oznaczenie znakiem usługowym ENERGY STAR lub spełniać kryteria efektywności energetycznej co najmniej równoważne z koniecznymi do uzyskania takiego oznaczenia. Zgodność z normą EPEAT. | |
| **32.** | **Oświadczenia** | Oświadczenie producenta, że w przypadku nie wywiązania się z obowiązków gwarancyjnych oferenta przejmie na siebie wszelkie zobowiązania związane z serwisem urządzeń.  Oświadczenie potwierdzające pochodzenie oferowanego sprzętu z oficjalnego polskiego kanału dystrybucji, podpisane przez producenta.  Serwis gwarancyjny oraz konserwacja urządzeń musi być świadczona przez organizację serwisową producenta lub firmę certyfikowaną przez producenta do świadczenia usług serwisowych, mającą swoją placówkę serwisową na terenie Polski. Dokumenty potwierdzające spełnienie ww. należy dołączyć do oferty. | |
| 1. **DRUKARKA ETYKIET – 2 SZT.** | | | |
|  | **PARAMETR** | **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE** | |
| **1.** | **Technologia druku** | Termotransferowy. | |
| **2.** | **Rozdzielczość druku** | Min. 203 dpi. | |
| **3.** | **Maksymalna szerokość druku** | Min. 100 mm. | |
| **4.** | **Maksymalna długość druku** | Min. 900 mm. | |
| **5.** | **Minimalna szerokość etykiety** | Min. 26 mm. | |
| **6.** | **Maksymalna szerokość etykiety** | Min. 108 mm. | |
| **7.** | **Minimalna długość etykiety** | Min. 9,5 mm. | |
| **8.** | **Maksymalna długość etykiety** | Min 900 mm. | |
| **9.** | **Prędkość druku** | Min. 100 mm/sekundę. | |
| **10.** | **Szerokość taśmy** | Co najmniej w zakresie 34 - 110 mm. | |
| **11.** |  | Wbudowany interfejs USB w wersji min. 2.0, dołączony przewód sygnałowy o długości min. 3m. | |
| **12.** | **Języki programowania** | EPL, ZPL. | |
| **13.** | **Obsługiwane kody kreskowe (co najmniej)** | 1D: Code 39, Code 128 (A, B or C user selectable/Auto select), UCC/EAN-128, Code 93, Codabar, Interleaved 2 of 5, UPC-A, UPC-E,UPC-A with 2 and 5 add on, Plessey, POSTNET, German Post, Japanese Postnet 2D: PDF-417, Macro PDF-417, Maxi Code (Modes 2, 3, 4, 6), QR Code. | |
| **14.** |  | Dołączony przewód zasilający i w przypadku wykorzystywania zasilacza zewnętrznego zasilacz musi być dołączony do urządzenia, odrywacz, instalacyjny dysk DVD-ROM lub pendrive ze sterownikami (TWAIN) i oprogramowaniem. | |
| **15.** | **Waga** | Max 2,5 kg. | |
| **16.** |  | Drukarka musi bez żadnego problemu współpracować z systemem elektronicznego zarządzania dokumentacja EZD PUW. | |
| **17.** |  | Urządzenia muszą być fabrycznie nowe, pochodzić z legalnego źródła, zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i świadczonych przez sieć serwisową producenta na terenie Polski | |
| **18.** | **Gwarancja** | Min. 2 lata gwarancji | |
|  | | | |
| **CZĘŚĆ II – DOSTAWA SPRZĘTU KOMPUTEROWEGO, SERWERA NAS ORAZ DYSKÓW DO SERWERA NAS - BACKUP PRZEZNACZONY DO SYSTEMU (EZD), URZĄDZENIA WIELOFUNKCYJNEGO ORAZ ZAPORY SIECIOWEJ UTM WRAZ Z 12 MIESIĘCZNĄ SUBSKRYPCJĄ** | | | |
| 1. **KOMPUTER ALL-IN-ONE Z PAKIETEM BIUROWYM – 11 szt.** | | | |
|  | **PARAMETR** | | **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE** |
| **1.** | **Typ** | | Komputer stacjonarny. Typu All in One, komputer fabrycznie wbudowany w obudowę monitora, nie dopuszcza się komputerów podłączanych do monitora w dedykowanych zatokach. |
| **2.** | **Procesor** | | Procesor wielordzeniowy posiadający min. 18MB pamięci podręcznej Cache dedykowany do pracy w komputerach stacjonarnych, osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 19600 pkt. według wyników opublikowanych na stronie <https://www.cpubenchmark.net/cpu_list.php> |
| **3.** | **Pamięć RAM** | | 16GB DDR4 3200MHz, jeden slot wolny. Możliwość rozbudowy do min 64GB. |
| **4.** | **Pamięć masowa** | | 512GB SSD M.2 NVMe.  Możliwość instalacji dodatkowego dysku twardego. |
| **5.** | **Karta graficzna** | | Zintegrowana. |
| **6.** | **Matryca** | | Matryca FHD (1920 x 1080) w rozmiarze min. 23.8”, z powłoką przeciwodblaskową o typowych parametrach nie gorszych niż:   * Jasność 250cd/m2; * Kontrast 1000:1; * Kąty widzenia matrycy 178 stopni (+/-89 stopni) poziomo oraz pionowo; |
| **7.** | **Wyposażenie multimedialne** | | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki min. 2W na kanał.  Wbudowana w obudowę matrycy cyfrowa kamera 2,0 MP. Mechanicznie chowana w obudowie (nie dopuszcza się kamer przekręcanych).  Wbudowane w obudowę dwa mikrofony. |
| **8.** | **Obudowa** | | Typu All-in-One zintegrowana z monitorem min. 23,8”. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki. Demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi. Komputer musi posiadać możliwość zainstalowania na ścianie przy wykorzystaniu ściennego systemu montażowego VESA 100.  Zasilacz wewnętrzny o mocy min. 160W o efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% (nie dopuszcza się zasilaczy zewnętrznych).  Zasilacz w oferowanym komputerze musi się znajdować na stronie <http://www.plugloadsolutions.com/80pluspowersupplies.aspx>  Wbudowany w obudowie wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji.  Podstawa jednostki typu All – in – One musi umożliwiać:  Regulację pochyłu pionowego w zakresie od -5 do 30 stopni.  Regulację wysokości w zakresie minimum 10 cm.  Ustawienie jednostki w trybie Pivot.  Obrót podstawy w lewą oraz prawą stronę. |
| **9.** | **Zdalne zarządzanie** | | Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca min.:   * Monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej; * Zdalną konfigurację ustawień BIOS; * Zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego; * Zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej; * Technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN (<http://www.dmtf.org/standards/wsman>) oraz DASH (<http://www.dmtf.org/standards/mgmt/dash/>) |
| **10.** | **Bezpieczeństwo** | | Płyta główna zawierająca układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego.  Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot’owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego.  Czujnik otwarcia obudowy, musi zbierać zdarzenia i zapisywać je w BIOS. |
| **11.** | **BIOS** | | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio.  Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie.  Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła systemowego/użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu hasła systemowego/użytkownika w BIOS jest wstanie zidentyfikować ustawienia oraz dokonać zmiany hasła systemowego/użytkownika. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość ustawienia portów USB w trybie „no BOOT” (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo.  Dedykowane pole inwentarzowe umożliwiająca wpisanie oznaczenia sprzętu. Pole po nadaniu numeru nie może być edytowalne.  Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS. |
| **12.** | **Certyfikaty i standardy** | | Certyfikat ISO9001 dla producenta sprzętu.  Deklaracja zgodności CE.  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001.  Certyfikat TCO Edge, wymagana certyfikacja na stronie: <http://tcocertified.com/product-finder/> .  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram. |
| **13.** | **Ergonomia** | | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy jałowej dysku twardego (IDLE) wynosząca maksymalnie 26 dB. |
| **14.** | **System operacyjny** | | Zainstalowany system operacyjny Windows 11 Professional, klucz licencyjny zapisany trwale w BIOS, umożliwiać reinstalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.  Parametry równoważności dla systemu operacyjnego:   1. Interfejs graficzny użytkownika pozwalający na obsługę:    1. Klasyczną przy pomocy klawiatury i myszy;    2. Dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych; 2. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim. 3. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe. 4. Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje. 5. Wbudowany system pomocy w języku polskim. 6. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. 7. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego. 8. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika. 9. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta z mechanizmem sprawdzającym, które z poprawek są potrzebne. 10. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 11. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 12. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 13. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 14. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). 15. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. 16. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. 17. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. 18. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe. 19. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 20. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu. 21. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. 22. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 23. Obsługa standard NFC (near field communication). 24. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 25. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 26. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 27. Mechanizmy uwierzytelniania w oparciu o:     1. login i hasło;     2. karty z certyfikatami (smartcard);     3. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM);     4. Wirtualnej tożsamości użytkownika potwierdzanej za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu. Mechanizm musi być ze specyfikacją FIDO; 28. Mechanizmy wieloskładnikowego uwierzytelniania. 29. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5. 30. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu. 31. Wsparcie dla algorytmów Suite B (RFC 4869). 32. Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji. 33. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku. 34. Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym. 35. Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny. 36. Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol 2.0. 37. Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji. 38. Możliwość konfiguracji trybu „kioskowego” dającego dostęp tylko do wybranych aplikacji i funkcji systemu. 39. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec. 40. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. 41. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 42. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń. 43. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 44. Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego. (provisioning). 45. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. 46. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. 47. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 48. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. 49. Udostępnianie wbudowanego modemu. 50. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 51. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 52. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 53. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). 54. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych. 55. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika. 56. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB. 57. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych. 58. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych. 59. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu. |
| **15.** | **Wymagania dodatkowe** | | Wbudowane porty:  1x DisplayPort++ 1.4/HDCP 2.3  1x HDMI In 1.4a  1 x HDMI Out 2.0  1x USB 3.2 Gen 2 Type-C port  5x USB 3.2 Type-A port  Wymagane porty USB wbudowane, nie dopuszcza się stosowania rozgałęziaczy, hub’ów itp. Wszystkie porty dostępne dla użytkownika w najniższej możliwej regulacji wysokości.  1x Universal audio jack  1x Line-out audio  1x RJ-45 port 10/100/1000 Mbps  Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, min. 2 złącza M.2 dla dysku twardego oraz 1 złącze M.2 karty WiFi.  Klawiatura USB w układzie polski programisty.  Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll). |
| **16.** | **Warunki gwarancji**  **Wsparcie techniczne** | | 3-letnia gwarancja producenta świadczona na miejscu u klienta. Czas reakcji serwisu - do końca następnego dnia roboczego.  Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. |
| **17.** | **Dodatkowe oprogramowanie** | | Oprogramowanie producenta komputera z nieograniczoną czasowo licencją na użytkowanie umożliwiające:  - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,  - sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi  - dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne  - włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji  - sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania)  - dostęp do wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml  - dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku \*.xml |
| **18.** | **Oprogramowanie biurowe** | | 1) Zamawiający wymaga dostarczenia licencji wieczystej oprogramowania w najnowszej na dzień składania ofert wersji, wyposażonego w następujące wbudowane funkcjonalności, bez użycia dodatkowych aplikacji:  a. dostępność pakietu w wersjach 32-bit oraz 64-bit, stały dostęp do najnowszych aktualizacji zakupionej wersji oprogramowania,  b. możliwość dostosowania dokumentów i szablonów do potrzeb użytkownika, oraz narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców.  2) Wymagania odnośnie interfejsu użytkownika:  a. pełna polska wersja językowa interfejsu użytkownika.  b. prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.  3) 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 ze zm.),  c. umożliwia kreowanie plików w formacie XML,  d. wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES.  4) W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).  5) Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.  6) Pakiet zintegrowanych aplikacji biurowych musi zawierać nieograniczone czasowo ani funkcjonalnie następujące składowe:  a. edytor tekstów.  b. arkusz kalkulacyjny.  c. narzędzie do przygotowywania i prowadzenia prezentacji.  d. narzędzie do zarządzania informacją prywatną.  Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  7) 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).  Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013, 2016, 2019, 365 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.  q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  8) Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:  a. przygotowywanie prezentacji multimedialnych, które będą:  - prezentowanie przy użyciu projektora multimedialnego  - drukowanie w formacie umożliwiającym robienie notatek  b. zapisanie jako prezentacja tylko do odczytu.  c. nagrywanie narracji i dołączanie jej do prezentacji.  d. opatrywanie slajdów notatkami dla prezentera.  e. umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.  f. umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.  g. odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.  h. możliwość tworzenia animacji obiektów i całych slajdów.  i. 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.  j. pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013, 2016, 2019 i 365.  9) narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:  a. pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.  b. przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.  c. filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.  d. tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.  e. automatyczne grupowanie poczty o tym samym tytule.  f. tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.  g. oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.  h. mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,  i. zarządzanie kalendarzem.  j. udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.  k. przeglądanie kalendarza innych użytkowników.  l. zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.  m. zarządzanie listą zadań.  n. zlecanie zadań innym użytkownikom.  o. zarządzanie listą kontaktów.  p. udostępnianie listy kontaktów innym użytkownikom.  q. przeglądanie listy kontaktów innych użytkowników.  r. możliwość przesyłania kontaktów innym użytkowników  s. możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http. |
| 1. **SERWER NAS Z OPROGRAMOWANIEM – 1 szt.** | | | |
|  | **PARAMETRY** | | **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE** |
| **1.** | **Typ urządzenia** | | Serwer NAS. |
| **2.** | **Obudowa** | | Rack. |
| **3.** | **Procesor** | | Ośmiordzeniowy procesor o taktowaniu bazowym 2,0 GHz, maksymalnie  2,7 GHz z technologią Turbo Boost osiągający w teście PassMark w terminie pomiędzy dniem zamieszczenia ogłoszenia na patformie zakupowej ROPS w Rzeszowie a terminem złożenia oferty co najmniej 9000 punktów. |
| **4.** | **Sprzętowy mechanizm szyfrowania** | | Tak (AES-NI). |
| **5.** | **Pamięć RAM** | | Min. 16 GB pamięci ECC UDIMM z możliwością rozszerzenia do min. 64 GB. |
| **6.** | **Możliwości rozbudowy** | | Sprzęt powinien być wyposażony w min. 12 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 36 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą gniazd rozszerzeń Infiniband. |
| **7.** | **Dyski twarde** | | Urządzenie główne musi być wyposażone w 10szt. dysków twardych SATA 3.5” tego samego producenta co urządzenie klasy korporacyjnej o pojemności min. 12 TB każdy. Średni czas do awarii (MTTF) musi wynosić min. 2.5 mln godzin. |
| **8.** | **Porty zewnętrzne** | | Minimum:   * 2 porty USB 3.2.1; * 2 gniazda rozszerzenia; |
| **9.** | **Porty sieciowe** | | Minimum:   * 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego); * 2 porty 10Gbe SFP+ (wykonawca dostarczy 2 kable DAC 10Gb SFP+); |
| **10.** | **Funkcja Wake on LAN/WAN** | | Tak. |
| **11.** | **Gniazdo rozszerzeń PCIe 3.0** | | Min. 2x 8-liniowe gniazdo x8 (Gen.3). |
| **12.** | **Wentylator obudowy** | | Min. 4 wentylatory 80 mm x 80 mm. |
| **13.** | **Obsługiwane protokoły sieciowe** | | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS  Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV. |
| **14.** | **Obsługiwane systemy plików** | | Min.:   * Wewnętrzny: Btrfs, ext4; * Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+; |
| **15.** | **Zarządzanie pamięcią masową** | | * Maksymalny rozmiar pojedynczego wolumenu: 108 TB /;   200 TB (wymagana pamięć RAM 32 GB);   * Minimalny liczba wewnętrznych wolumenów: 128; * Minimalny liczba obiektów iSCSI Target: 256; * Minimalny liczba jednostek iSCSI LUN: 512;   Obsługa klonowania/migawek jednostek iSCSI LUN; |
| **16.** | **Obsługiwane typy macierzy RAID** | | Synology RAID F1, Podstawowy (Basic), JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10. |
| **17.** | **Funkcja udostępniania plików** | | * Minimalna liczba kont użytkowników: 16 000; * Minimalna liczba grup użytkowników: 512; * Minimalna liczba folderów współdzielonych: 512; * Minimalna liczba jednoczesnych połączeń CIFS/AFP/FTP: 2000; |
| **18.** | **Uprawnienia** | | Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL). |
| **19.** | **Wirtualizacja** | | Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack®. |
| **20.** | **Usługa katalogowa** | | Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP. |
| **21.** | **Bezpieczeństwo** | | Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania). |
| **22.** | **Obsługiwane systemy klienckie** | | Windows® 7 i nowsze, macOS® 10.12 i nowsze. |
| **23.** | **Obsługiwane przeglądarki** | | Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach. |
| **24.** | **Zasilanie** | | Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz. |
| **25.** | **Oprogramowanie** | | * Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych; * Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów; * Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym; * Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia; |
| **26.** | **Konserwacja** | | * Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack dostarczonych z zestawem; * Wymiana modułu zasilacza ma przebiegać w szybki i bezpieczny sposób bez wyłączania urządzenia oraz bez użycia narzędzi; |
| **27.** | **Gwarancja** | | Wykonawca udzieli gwarancji:   * 5 lat na urządzenia główne; * 5 lat gwarancji na dyski twarde; |
| **28.** | **Warunki dodatkowe** | | Wykonawca zainstaluje fizycznie dostarczony serwer NAS w szafie zamawiającego, przeprowadzi konfigurację według wytycznych Zamawiającego oraz dokona przeszkolenia pracownika Zamawiającego. |
| 1. **URZĄDZENIE WIELOFUNKCYJNE LASEROWE KOLOROWE A3 – 1 SZT.** | | | |
|  | **PARAMETRY** | | **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE** |
| **1.** | **Typ urządzenia** | | urządzenie wielofunkcyjne: drukarka kolorowa, kopiarka kolorowa, skaner kolorowy. |
| **2.** | **Prędkość druku** | | mono i kolor min. 25 stron A4 na minutę;  min. 15 stron A3 na minutę; |
| **3.** | **Technologia druku** | | laserowa kolorowa C,M,Y,K. |
| **4.** | **Panel dotykowy/ rozdzielczość** | | Panel dotykowy o minimalnej przekątnej 10,1” oraz rozdzielczości 1024 x 600 personalizowany w języku polskim, z możliwością wyświetlania interfejsów zewnętrznych aplikacji np. do zarządzania wydrukiem, systemów OCR. |
| **5.** | **Maksymalny format papieru** | | nie mniejszy niż SRA3, możliwość wydruku banderowego. |
| **6.** | **Czas nagrzewania** | | nie więcej niż 13 sekundy. |
| **7.** | **Czas wykonania pierwszej kopii** | | nie więcej niż 5,2 sekund mono, nie więcej niż 6,9 sekundy kolor. |
| **8.** | **Wejściowa obsługa papieru** | | co najmniej 2 kasety uniwersalne o pojemności nie mniejszej niż 500 arkuszy każda, taca ręczna o pojemności nie mniejszej niż 150 arkuszy. |
| **9.** | **Obsługiwana gramatura papieru** | | co najmniej w zakresie od 52 do 300 g/m2. |
| **10.** | **Automatyczny podajnik dokumentów** | | wymagany, z funkcją odwracania, o pojemności nie mniejszej niż 100 arkuszy, obsługujący formaty A6-A3; w gramaturze 35-128 g/m². |
| **11.** | **Prędkość skanowania** | | Min. 80 oryginałów/min. (300 dpi) zarówno w kolorze jak i w mono. |
| **12.** | **Funkcja zoom** | | co najmniej w zakresie od 25-400% w odstępach 0.1% ; automatyczne powiększenie. |
| **13.** | **Zużycie Energii** | | 220–240 V / 50/60 Hz; o mocy 1,58 kW TEC Value 0.9KWh. |
| **14.** | **Kopiowanie wielokrotne** | | co najmniej w zakresie 1 - 9,999. |
| **15.** | **Zainstalowana pamięć** | | min. 8,0 GB RAM oraz twardy dysk SSD o pojemności min. 250 GB. |
| **16.** | **Język drukarki** | | PCL 6; PCL 5c; PostScript 3 (CPSI 3016); XPS. |
| **17.** | **Zawansowane funkcje drukowania** | | Aplikacja która umożliwia drukowanie z pozycji komputera bez instalacji sterownika za pomocą „przeciąg i puść”. Umożliwiająca:   * Tworzenie Hot folderów do bezpośredniego druku; * Skojarzenie specyficznych ustawień z hot folderami; * Automatyczne zapisywanie plików w folderach „druku”; * Obsługuje PDF, TIFF, PCL i PS; |
| **18.** | **Protokoły sieciowe** | | TCP/IP (IPv4/IPv6); SMB; LPD; IPP; SNMP; HTTP(S); AppleTalk; Bonjour. |
| **19.** | **Rozdzielczość kopiowania i skanowania** | | nie mniejsza niż 600 x 600 dpi. |
| **20.** | **Rozdzielczość drukowania** | | Nie mniejsza niż 1,800 x 600 - 1,200 x 1,200. |
| **21.** | **Interfejsy** | | USB 2.0, 10/100/1000BaseTX. |
| **22.** | **Funkcje drukarki** | | bezpośredni druk PDF, bezpośredni druk z pamięci USB. |
| **23.** | **Tryby skanera** | | Kolorowy sieciowy z możliwością skanowania:   * Skanowania na adres e-mail (Scan-to-Me); * Skanowanie do SMB (Scan-to-Home); * Skanowanie do FTP; * Skanowanie do skrzynki (HDD); * Skanowanie do USB; * Skanowanie do WebDAV; * Skanowanie do DPWS; * Skanowanie sieciowe TWAIN; |
| **24.** | **Wyjściowe formaty plików skanera** | | JPEG; TIFF; PDF; PDF/A; kompaktowy PDF; szyfrowany PDF; przeszukiwany PDF ; XPS; kompaktowy XPS; PPTX; DOCX, XLSX, RTF,TXT. |
| **25.** | **Szafka pod urządzenie** | | Wymagana, metalowa na kółkach. Zamawiający wymaga szafki w kolorach odpowiadającym kolorom urządzenia. |
| **26.** | **Funkcje monitorująco raportujące** | | Aplikacja umożliwiająca po przez przeglądarkę internetową, dodawanie użytkowników (do 1000 kont użytkowników; obsługa również Active Directory (login + hasło + e-mail + katalog SMB)) z możliwością definiowania uprawnień do danych funkcji urządzenia np. Wydruku: mono / kolor, Kopia Mono / Kolor Skanowanie.  Rozwiązanie winno umożliwiać również możliwość raportowania ilości wykonanych wydruków / kopii / skanów, poszczególnych użytkowników wpisanych do systemu. System musi posiadać autoryzacje użytkowania na maszynie za pomocą: Kodu PIN. |
| **27.** | **Wymagane funkcje bezpieczeństwa** | | ISO 15408 Common Criteria (w trakcie oceny); Filtrowanie IP i blokowanie portów; Komunikacja sieciowa SSL2; SSL3 i TLS1.0/1.1/1.2; Obsługa IPsec; Obsługa IEEE 802.1x;  Uwierzytelnianie użytkowników; Dziennik uwierzytelniania;  Bezpieczny wydruk; Kerberos; Nadpisywanie dysku twardego (min. 8 standardowych metod); Szyfrowanie danych na twardym dysku (AES 256); Automatyczne usuwanie danych z pamięci;  Odbiór faksów poufnych;  Szyfrowanie danych użytkownika drukarki;  Skanowanie antywirusowe w czasie rzeczywistym, Ochrona przed kopiowaniem (Copy Guard, Password Copy) |
| **28.** | **Materiały eksploatacyjne** | | Toner czarny dostarczony z urządzeniem pozwalający na wydrukowanie minimum 28.000 stron A4 przy zadruku 5% oraz tonery cyan, magenta, yellow dostarczone z urządzeniem pozwalające na wydrukowanie minimum 28.000 stron A4 przy zadruku 5%. |
| **29.** | **Certyfikaty** | | EDS, EAC, NEMKO, EMC, DoC, ISO 9001, ISO 14001, Blue Angel Mark, TUV |
| **30.** | **Instalacja** | | Zamawiający wymaga w cenie uruchomienia wyżej opisanego urządzenia oraz wdrożenia systemów zawansowanych funkcji drukowania oraz skanowania w skazanym miejscu przez Zamawiającego. |
| **31.** | **Wymagania gwarancji** | | 3 lata gwarancji producenta urządzenia na miejscu u klienta, lub autoryzowanego przedstawiciela producenta posiadającego uprawnienia do napraw gwarancyjnych. |
| **32.** | **Oświadczenia** | | Oświadczenie bezpośredniego przedstawiciela producenta oferowanego sprzętu w Polsce, że w przypadku nie wywiązania się z obowiązków gwarancyjnych wykonawcy lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem gwarancyjnym dotyczącym urządzeń wielofunkcyjnych. |
| 1. **ZAPORA SIECIOWA UTM WRAZ Z 12 MIESIĘCZNĄ SUBSKRYPCJĄ – 1 SZT.** | | | |
|  | **PARAMETRY** | | **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE** |
| **1.** | **Wymagania ogólne** | | System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. |
| **2.** | **System wspiera protokoły IPv4 oraz IPv6** | | * Firewall; * Ochrony w warstwie aplikacji; * Protokołów routingu dynamicznego; |
| **3.** | **Redundancja, monitoring i wykrywanie awarii** | | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |
| **4.** | **Interfejsy, dysk, zasilanie:** | | 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:  * 10 portami Gigabit Ethernet RJ-45.  1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System jest wyposażony w zasilanie AC. |
| **5.** | **Funkcje systemu bezpieczeństwa:** | | W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |
| **6.** | **Polityki, Firewall** | | 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  * Translację jeden do jeden oraz jeden do wielu; * Dedykowany ALG (Application Level Gateway) dla protokołu SIP;  1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.  * Amazon Web Services (AWS); * Microsoft Azure; * Cisco ACI; * Google Cloud Platform (GCP); * OpenStack; * VMware NSX; * Kubernetes; |
| **7.** | **Połączenia VPN** | | 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:  * Wsparcie dla IKE v1 oraz v2; * Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM); * Obsługa protokołu Diffie-Hellman grup 19, 20; * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh; * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site; * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności; * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego; * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat; * Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu; * Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu; * Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth; * Mechanizm „Split tunneling” dla połączeń Client-to-Site.  1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:  * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0; * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta; * Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji; |
| **8.** | **Routing i obsługa łączy WAN** | | W zakresie routingu rozwiązanie zapewnia obsługę:   1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |
| **9.** | **Funkcje SD-WAN** | | 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| **10.** | **Zarządzanie pasmem** | | 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |
| **11.** | **Ochrona przed malware** | | 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie  z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| **12.** | **Ochrona przed atakami** | | 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 5. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 6. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |
| **13.** | **Kontrola aplikacji** | | 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 3. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 4. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 5. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 6. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |
| **14.** | **Kontrola WWW** | | 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |
| **15.** | **Uwierzytelnianie użytkowników w ramach sesji** | | 1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu; * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP; * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych;  1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| **16.** | **Zarządzanie** | | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |
| **17.** | **Logowanie** | | 1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |
| **18.** | **Certyfikaty** | | Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:   * ICSA lub EAL4 dla funkcji Firewall. |
| **19.** | **Gwarancja oraz wsparcie** | | 1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. 12 miesięcy. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie w trybie 24x7. 2. W ramach dostawy Wykonawca zainstaluje, oraz skonfiguruje dostarczone urządzenie według wytycznych Zamawiającego. |

|  |  |  |  |
| --- | --- | --- | --- |
| **CZĘŚĆ III – DOSTAWA AKCESORII ELEKTRONICZNYCH I KOPUTEROWYCH** | | | |
| **AKCESORIA KOMPUTEROWE I ELEKTRONICZNE** | | | |
|  | **PARAMETRY** | **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE** | |
| **1.** | **Patchcord dł. 0,5m** | - Standard skrętki – Cat 6  - Rodzaj połączenie – kabel prosty zgodny ze standardem T568B  - Kabel sieciowy miedziany obustronnie zakończony jest wtykami RJ45 (8P8C) – męskie  - Końcówki kabla wyposażone w odgiętkę i ochronę zatrzasku.  - Oznaczenie długości na płaszczu kabla  - Fabrycznie zalewane wtyki  - Ekranowanie (brak): U/UTP  - Struktura: 4x 26/7 AWG, skrętka  - Płaszcz: PVC  - Pozłacane styki  - Powłoka żył: HD-PE  - Temp. Pracy: od -20°C do 60°C | **40 szt.** |

|  |  |  |  |
| --- | --- | --- | --- |
| **2.** | **Patchcord dł. 1m** | - Standard skrętki – Cat 6  - Rodzaj połączenie – kabel prosty zgodny ze standardem T568B  - Kabel sieciowy miedziany obustronnie zakończony jest wtykami RJ45 (8P8C) – męskie  - Końcówki kabla wyposażone w odgiętkę i ochronę zatrzasku.  - Oznaczenie długości na płaszczu kabla  - Fabrycznie zalewane wtyki  - Ekranowanie (brak): U/UTP  - Struktura: 4x 26/7 AWG, skrętka  - Płaszcz: PVC  - Pozłacane styki  - Powłoka żył: HD-PE  - Temp. Pracy: od -20°C do 60°C | **40 szt.** |

|  |  |  |  |
| --- | --- | --- | --- |
| **3.** | **Patchcord dł. 3m** | - Standard skrętki – Cat 6  - Rodzaj połączenie – kabel prosty zgodny ze standardem T568B  - Kabel sieciowy miedziany obustronnie zakończony jest wtykami RJ45 (8P8C) – męskie  - Końcówki kabla wyposażone w odgiętkę i ochronę zatrzasku.  - Oznaczenie długości na płaszczu kabla  - Fabrycznie zalewane wtyki  - Ekranowanie (brak): U/UTP  - Struktura: 4x 26/7 AWG, skrętka  - Płaszcz: PVC  - Pozłacane styki  - Powłoka żył: HD-PE  - Temp. Pracy: od -20°C do 60°C | **10 szt.** |

|  |  |  |  |
| --- | --- | --- | --- |
| **4.** | **Wtyk RJ45 – 8P8C** | - Standard wtyku – min. 5e  - Obudowa wtyku – przeźroczysta  - Przeznaczenie – uniwersalne, montaż na skrętce typu drut  - Pozłacane kontakty złącz | **100 szt.** |

|  |  |  |  |
| --- | --- | --- | --- |
| **5.** | **Dysk wewnętrzny SSD** |  | |
| Rodzaj dysku | SSD | **10 szt.** |
| Pojemność dysku | Min. 512 GB |
| Typ dysku | Wewnętrzny |
| Format | 2.5” |
| Interfejs | SATA III (6 Gb/s0\) |
| Maksymalna prędkość odczytu [MB/s] | min. 550 |
| Maksymalna prędkość zapisu [MB/s] | min. 490 |
| Rodzaj pamięci | Flash NAND 3D |
| Gwarancja | 36 miesięcy |

|  |  |  |  |
| --- | --- | --- | --- |
| **6.** | **Telefon bezprzewodowy** |  | |
| Funkcje | GAP - Kompatybilny  Wiele słuchawek - 6  Czysty dźwięk - Tak  Tryb One Touch Eco - Tak | **5 szt.** |
| Słuchawka | Ulepszenie głosu - Tak  Klawisz nawigacyjny - Tak  Podświetlona klawiatura - Tak  Tryb głośno mówiący - Tak  Sygnalizacja LED - Tak  Powtarzanie ostatnio wybieranego numeru - Tak  Pamięć numerów wybieranych - min. 10 (imię i numer)  Funkcja wycisz - Tak |
| Identyfikacja numeru abonenta wywołującego | Prezentacja numeru aboneneta wywołującego – Tak Rejestr połączeń - Tak |
| Książka telefoniczna | Min. liczba wpisów - 120 wpisów (imię i numer) |
| Dzwonek | Liczba melodii dzwonka - min. 30  Liczba sygnałów dzwonka - min. 10  Poziomy dzwonka - Tak, min. 7 kroków |
| Poziomy głośnik dzwonka | Min. 6 poziomów + "wyłączony" |
| LCD | Rodzaj LCD - min. 1.8 calowy monochromatyczny, min. 103x65 pikseli  Podświetlany LCD - Biały |
| Zegar | Data i Czas - Tak  Alarm - Tak |
| Restrykcje połączeń | Tak |
| Połączenie konferencyjne | Tak |
| Blokada klawiatury | Tak |
| Odbiór dowolnym klawiszem | Tak |
| Menu w języku polskim | Tak |
| Tryb nocny | Tak |
| Regulacja głośności słuchawki | min. 4 kroki |
| Akumulator | Typ baterii - akumulatory Ni-MH (2 x AAA)  Czas ładowania - max. 7 godzin  Czas oczekiwania - do 170 godzin |
| Czas rozmowy | do 15 godzin |
| Gwarancja | min. 12 miesięcy |

|  |  |  |  |
| --- | --- | --- | --- |
| **7.** | **Pendrive 64GB USB 3.0** |  | |
| Pojemność | 64 GB | **5 szt.** |
| Interfejs | USB 3.1 Gen. 1 (USB 3.0) |
| Dodatkowe informacje | Wstrząsoodporność |
| Gwarancja | 60 miesięcy (producenta) |

|  |  |  |  |
| --- | --- | --- | --- |
| **8.** | **Czytnik kart pamięci** |  | |
| Typ czytnika | Zewnętrzna | **3 szt.** |
| Łączność | Przewodowa |
| Interfejs | USB 3.0 |
| Obsługiwane karty pamięci | SD, Micro SD, CompactFlash |
| Prędkość transmisji danych | Do 5 Gbit/s |
| Dodatkowe informacje | Hot Swap, Plug & Play, aluminiowa obudowa |
| Gwarancja | min. 24 miesiące (producenta) |