Spis treści



**UWAGA!**

**Niniejszy załącznik określa minimalne wartości parametrów technicznych i funkcjonalnych sprzętu oraz oprogramowania. W podanych przez Zamawiającego pozycjach, gdzie stosuje się ilość, wymiar, ciężar, grubość itd., Zamawiający określa wymogi jako niezbędne minimum.**

**INSTRUKCJA WYPEŁNIANIA PONIŻSZYCH TABEL!**

**W poniższych tabelach należy wypełnić pola oznaczone kolorem żółtym ..... . Ponadto w miejscach oznaczonych „Tak*/Nie*" należy skreślić niepotrzebną odpowiedź.**

**W przypadku niewypełnienia wymaganego pola lub braku skreślenia niepotrzebnej odpowiedzi przyjmuje się, że Wykonawca nie oferuje sprzętu oraz oprogramowania spełniającego wymagania określone w Opisie Przedmiotu Zamówienia.**



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

## 1. Komputer stacjonarny – 43 szt.

| Lp. | Nazwa komponentu | Wymagane parametry techniczne komputerów | Oferowane parametry techniczne |
|---|---|---|---|
| 1. | Typ | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta. | Producent: ……<br>Model: ……<br>Symbol: ……<br>Zamawiający wymaga dołączenia do oferty dokumentów:<br>Karty katalogowe wraz ze specyfikacją. |
| 2. | Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. | Spełnia Tak*/Nie* |
| 3. | Procesor | SYSmark 25 PerformanceTest:<br>Overall Rating – **co najmniej wynik 1600 punktów - wyniki załączyć do oferty.**<br>Wymagane testy wydajnościowe Wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).<br>Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Wykonawca w przypadku wątpliwości, wykonawca na ewentualne wezwanie musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego. | Spełnia Tak*/Nie* |
| 4. | Płyta główna | Musi posiadać:<br>- zintegrowaną kartę dźwiękową, kartę sieciową Wi-Fi 5 (802.11 a/b/g/n/ac), kartę sieciową LAN 10/100/1000 Mbps, moduł Bluetooth,<br>- złącza zewnętrzne: USB 2.0 – min 4 szt., USB 3.2 Gen.1 – min 2 szt., wyjście słuchawkowe/wejście mikrofonowe - 1 szt. **HDMI - 1 szt., Display Port - 1 szt.,**<br>- złącza wewnętrzne (wolne) PCI-e x16 – 1 szt., PCI-e x1 - 1 szt., SATA III - 1 szt.,<br>- wbudowany moduł TPM | |
| 5. | Pamięć RAM | Minimum 16GB DDR4 2666MHz. Możliwość rozbudowy do min 64GB. | Spełnia Tak*/Nie* |
| 6. | Pamięć masowa | Dysk M.2 SSD minimum 256GB PCIe NVMe | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | Obudowa musi umożliwiać montaż min. trzech dysków SATA. | |
| 7. | Wydajność grafiki | Zintegrowana karta graficzna osiągająca w teście SYSmark 25 Creativity **co najmniej 1300 punktów - wyniki załączyć do oferty.** | Spełnia Tak*/Nie*<br>Zamawiający wymaga dołączenia do oferty dokumentów:<br>Wynik testu aplikacyjnego SYSmark 25 Creativity:<br>Overall Rating:<br>…… |
| 8. | Obudowa | Obudowa typu Small Factor Form. Umożliwiająca montaż 1x dysku 3.5" lub 1x dysku 2.5" wewnątrz obudowy. Napęd optyczny zamontowany w dedykowanej wnęce zewnętrznej 5.25" typu slim. Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. | Spełnia Tak*/Nie* |
| 9. | System operacyjny | System operacyjny: Windows 11 Pro (język polski) lub równoważny (kryteria równoważności: bezpieczeństwo, stabilność i wydajność wraz z obsługą: Active Directory, szczególnie pełna wsparcie AD Group Policy i Folder Redirection oraz .NET Framework 4.5).<br>System operacyjny musi pozwalać na uruchomienie programów komputerowych użytkowanych w ramach infrastruktury zamawiającego, bez dodatkowego nakładu na wdrożenie, instalację i szkolenia.<br>System może być integralną częścią zestawu komputerowego, spełniającą powyższe wymagania.<br>Zaoferowany sprzęt musi posiadać certyfikat zgodności z zainstalowanym system operacyjnym. | Producent<br>……..<br><br>Nazwa i wersja oprogramowania<br>……..<br>Spełnia Tak*/Nie* |
| 10. | Oprogramowanie zabezpieczające | Oprogramowanie zabezpieczające klasy EDR (Endpoint Detection and Response), centralnie zarządzane przez przeglądarki internetowe, serwer zarządzający w chmurze. Oprogramowanie powinno zawierać moduły/funkcje:<br>- zawansowane (tradycyjna, heurystyczna) ochrona antywirusowa, malware i przed innym szkodliwym oprogramowaniem, także ze wsparciem sztucznej inteligencji i usługami chmurowymi,<br>- ochrona ruchu internetowego i przeglądarek internetowych, kontrola treści, anty-phishing,<br>- zaawansowana zapora sieciowa oparta o zasady, z kontrolą połączeń, listą blokowanych i zabronionych adresów internetowych,<br>- ochrony danych i monitoring przed zagrożeniami ransomware, szyfrowaniem i wyciekiem danych<br>- wsparcie dla systemów operacyjnych Windows, Linux, Mac,<br>- skanowanie i wykrywanie podatności w sieci komputerowej wraz z centralnym zarządzaniem,<br>- spełniać wymagania dotyczące zgodności ze standardem PCI DSS,<br>- skanowania i wykrywania umożliwiają wykrycie wszystkich hostów i urządzeń sieciowych w infrastrukturze, | Producent<br>……..<br><br>Nazwa i wersja oprogramowania<br>……..<br>Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | Oprogramowanie zabezpieczające musi posiadać certyfikaty: **VB100%, OPSWAT, AVLAB+++, AV Comperative Advance+**<br><br>Oprogramowanie zabezpieczające z licencją ważną minimum 12 miesięcy z możliwością przedłużenia | |
| 11. | Certyfikaty i standardy | Certyfikat ISO 9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)<br>Deklaracja zgodności CE (załączyć do oferty)<br>Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001<br>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. | Zamawiający wymaga dołączenia do oferty dokumentów:<br>Certyfikat ISO 9001 dla producenta sprzętu<br>Deklaracja zgodności CE<br>Potwierdzenie spełnienia kryteriów środowiskowych – zgodność z dyrektywą RoHS<br>Spełnia Tak*/Nie* |
| 12. | Warunki gwarancji | Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.<br>Minimalny czas trwania wsparcia technicznego producenta wynosi **12 m-cy**<br>Sposób realizacji usług wsparcia technicznego:<br>• Telefoniczne zgłaszanie usterek w dni robocze w godzinach 8-17.<br>• Dedykowany bezpłatny portal online producenta do zgłaszania usterek i zarządzania zgłoszeniami serwisowymi.<br>• Opcjonalna pomoc techniczna za pośrednictwem czat online.<br>Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii.<br>W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na miejsce wskazane przez klienta na następny dzien roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego.<br>Możliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń z nieaktywnym wsparciem technicznym. | **Pozycja podlegająca kryterium oceny ofert**<br><br>Zamawiający wymaga dołączenia do oferty dokumentów:<br>Certyfikat ISO 9001 na świadczenie usług serwisowych<br>Oświadczenie Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

## 2. Pakiet **biurowy** – 43 licencje

| Lp | Minimalne wymagania | Oferowane parametry |
|---|---|---|
| | Producent / Nazwa | Producent:<br>.....<br>Nazwa i wersja oprogramowania:<br>..... |
| | **Wymagania ogólne** | |
| 1. | Pakiet zintegrowanych aplikacji biurowych zawierający minimum:<br>- edytor tekstów,<br>- arkusz kalkulacyjny,<br>- narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami). | Spełnia Tak*/Nie* |
| 2. | Oprogramowanie musi być dostarczone z licencją bezterminową umożliwiającą odczytywanie, edytowanie i zapisywanie dokumentów lokalnie w jednym miejscu lub na wolumenach udostępnionych przez administratora systemu informatycznego. Dostarczona licencja musi umożliwiać bezpłatne pobranie pakietu ze strony producenta dostarczonego rozwiązania.<br>Nie dopuszcza się licencji typu refurbished. | |
| 3. | Pełna polska wersja językowa interfejsu użytkownika. | |
| 4. | Dostępna dokumentacja użytkownika w języku polskim. | |
| 5. | Musi umożliwiać instalację na dostarczonym systemie operacyjnym. | |
| 6. | Obsługa odczytu oraz zapisywania dokumentów w formatach minimum pdf, bmp, gif, jpg, png. | |
| 7. | Obsługa odczytu oraz zapisywania dokumentów w formatach minimum doc, docx, odt, rtf, txt, html. | |
| 8. | Obsługa odczytu oraz zapisywania dokumentów w formatach minimum xls, xlsx, ods, csv. | |
| 9. | Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) - użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się. Pełna integracja z AD Group Polisy | |
| 10. | Dokumenty muszą być tworzone zgodnie z zdefiniowanym układem informacji w postaci XML zgodnie z Tabelą B1 załącznika 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 (t.j. Dz.U.2017.2247). | |
| 11. | Wsparcie podpisu cyfrowego zgodnie z Tabelą A. 1.1 załącznika 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 (t.j. Dz.U.2017.2247). | |
| 12. | Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. | |
| | **EDYTOR TEKSTÓW** | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | |
|---|---|---|
| 1. | Edycja i formatowanie tekstu w języku polskim. | Spełnia Tak*/Nie* |
| 2. | Musi posiadać narzędzia sprawdzające pisownię i poprawność gramatyczną oraz funkcjonalność słownika wyrazów bliskoznacznych i autokorekty. | |
| 3. | Wstawianie oraz formatowanie tabel. | |
| 4. | Wstawianie oraz formatowanie obiektów graficznych. | |
| 5. | Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). | |
| 6. | Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. | |
| 7. | Automatyczne tworzenie spisów treści. | |
| 8. | Formatowanie nagłówków i stopek stron. | |
| 9. | Określenie układu strony (pionowa/pozioma). | |
| 10. | Wydruk dokumentów. | |
| **ARKUSZ KALKULACYJNY** | | |
| 1. | Tworzenie raportów tabelarycznych. | Spełnia Tak*/Nie* |
| 2. | Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych. | |
| 3. | Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe ora formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. | |
| 4. | Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice). | |
| 5. | Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. | |
| 6. | Wyszukiwanie i zamiana danych. | |
| 7. | Wykonywanie analiz danych przy użyciu formatowania warunkowego. | |
| 8. | Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. | |
| 9. | Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. | |
| 10. | Formatowanie czasu, daty i wartości finansowych z polskim formatem. | |
| 11. | Zapis wielu arkuszy kalkulacyjnych w jednym pliku. | |
| **NARZĘDZIE DO ZARZĄDZANIA INFORMACJĄ PRYWATNĄ (POCZTĄ ELEKTRONICZNĄ, KALENDARZEM, KONTAKTAMI I ZADANIAMI)** | | |
| 1. | Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego. | Spełnia Tak*/Nie* |
| 2. | Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych. | |
| 3. | Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców. | |
| 4. | Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną. | |
| 5. | Automatyczne grupowanie poczty o tym samym tytule. | |
| 6. | Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy. | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | |
|---|---|---|
| 7. | Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów. | |
| 8. | Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie. | |
| 9. | Zarządzanie kalendarzem. | |
| 10. | Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników. | |
| 11. | Przeglądanie kalendarza innych użytkowników. | |
| 12. | Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach. | |
| 13. | Zarządzanie listą zadań. | |
| 14. | Zlecanie zadań innym użytkownikom. | |
| 15. | Zarządzanie listą kontaktów. | |
| 16. | Udostępnianie listy kontaktów innym użytkownikom. | |
| 17. | Przeglądanie listy kontaktów innych użytkowników. | |
| 18. | Możliwość przesyłania kontaktów innym użytkowników. | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

## 3. Urządzenia wielofunkcyjne – 14 szt.

| Lp. | Nazwa komponentu | Wymagane parametry techniczne | Oferowane parametry techniczne |
|---|---|---|---|
| 1. | Typ drukarki | Mono | Producent: ……<br>Model: ……<br>Zamawiający wymaga dołączenia do oferty dokumentów:<br>Karta produktu |
| 2. | Funkcje | Drukowanie, Kopiowanie i skanowanie, Faksowanie | Spełnia Tak*/Nie* |
| 3. | Wyświetlacz | Kolorowy ekran dotykowy | Spełnia Tak*/Nie* |
| 4. | Maksymalny rozmiar papieru | A4 | Spełnia Tak*/Nie* |
| 5. | Pamięć | Nie mniej 256 MB | Spełnia Tak*/Nie* |
| 6. | Technologia | Laserowa | Spełnia Tak*/Nie* |
| 7. | Rozmiar wyświetlacza | Nie więcej 12.3 cm | Spełnia Tak*/Nie* |
| 8. | Połączenie | Sieć przewodowa, Sieć bezprzewodowa | Spełnia Tak*/Nie* |
| 9. | Interfejs sieci przewodowej | Ethernet (10Base-T/100Base-TX/) | Spełnia Tak*/Nie* |
| 10. | Interfejs sieci bezprzewodowej | IEEE 802.11b/g/n | Spełnia Tak*/Nie* |
| 11. | Lokalny interfejs | Hi-Speed USB 2.0 | Spełnia Tak*/Nie* |
| 12. | Kopiowanie dwustronne | Tak | Spełnia Tak*/Nie* |
| 13. | Rozdzielczość | Nie mniej 1200 x 600 dpi | Spełnia Tak*/Nie* |
| 14. | Rozmiar | Nie więcej niż 436 x 428 x 487 mm | Spełnia Tak*/Nie* |
| 15. | Waga | Nie większa niż 16.5 kg | Spełnia Tak*/Nie* |
| 16. | Poziom hałasu | Nie więcej niż Drukowanie 55dBA, tryb cichy 53dBA, tryb gotowości 36dBA | Spełnia Tak*/Nie* |
| 17. | Automatyczne faksowanie dwustronne | Tak | Spełnia Tak*/Nie* |
| 18. | Faks-modem | 33.6 kb/s | Spełnia Tak*/Nie* |
| 19. | Faks internetowy | Tak | Spełnia Tak*/Nie* |
| 20. | PC Fax | Tak | Spełnia Tak*/Nie* |
| 21. | Zawartość | Przewód zasilający, przewodnik bezpieczeństwa produktu, dysk z oprogramowaniem, karta gwarancyjna, podręcznik szybkiej obsługi | Spełnia Tak*/Nie* |
| 22. | Typy i gramatury | Standardowy i opcjonalny podajnik – zwykły, makulaturowy (pomiędzy 60 - 120gsm). Podajnik wielofunkcyjny - zwykły, makulaturowy (pomiędzy 60 - 200gsm). Drukowanie dwustronne - zwykły, makulaturowy (pomiędzy 60 - 105gsm) | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| 23. | Rozmiary | Standardowy podajnik - A4, Letter, A5, A5(Long Edge), A6, Executive, Legal, Folio, Mexico Legal, India Legal. Opcjonalny podajnik - A4, Letter, A5, Executive, Legal, Folio, Mexico Legal, India Legal. Podajnik wielofunkcyjny - szerokość: 76.2mm to 215.9mm x długość: 127mm to 355.6mm. Drukowanie dwustronne – A4. Automatyczny podajnik dokumentów (ADF) - szerokość: 105mm do 215.9mm x długość: 147.3mm to 355.6mm | Spełnia Tak*/Nie* |
| 24. | Obsługiwane | Windows®: Windows 10®, Windows® 8, Windows® 7, Windows Vista®, Windows® XP Professional, Windows® XP Home Edition, Windows® Server 2012R2, Windows® Server 2012, Windows® Server 2008R2, Windows® Server 2008, Windows® Server 2003 | Spełnia Tak*/Nie* |
| 25. | Wejście papieru | Podajnik papieru – 250 arkuszy, Podajnik wielofunkcyjny – 50 arkuszy, Automatyczny podajnik dokumentów (ADF) – 50 arkuszy | Spełnia Tak*/Nie* |
| 26. | Wyjście papieru | Zadrukiem do dołu - 150 arkuszy, Zadrukiem do góry (Prosta ścieżka papieru) - 1 arkusz | Spełnia Tak*/Nie* |
| 27. | Szybkość drukowania dwustronnego A4 | Do 20 obrazów na minutę | Spełnia Tak*/Nie* |
| 28. | Standardowa szybkość drukowania A4 | Do 40 stron na minutę | Spełnia Tak*/Nie* |
| 29. | Automatyczne drukowanie dwustronne | Tak | Spełnia Tak*/Nie* |
| 30. | Emulacje | PCL6, Postscript®3™, IBM Proprinter XL, Epson FX-850, PDF Version 1.7, XPS Version 1.0 | Spełnia Tak*/Nie* |
| 31. | Czas wykonania pierwszego wydruku | Mniej niż 7.2 sekundy | Spełnia Tak*/Nie* |
| 32. | Rozdzielczość | do 1,200 x 1,200dpi | Spełnia Tak*/Nie* |
| 33. | Skanowanie dwustronne | Skanowanie dwustronne | Spełnia Tak*/Nie* |
| 34. | Typ skanera | Podwójny CIS | Spełnia Tak*/Nie* |
| 35. | Rozdzielczość | do 1,200 x 1,200dpi (z szyby), 600 x 600dpi (ADF), 19,200 x 19,200dpi (Interpolowana) | Spełnia Tak*/Nie* |
| 36. | Szybkość | Mono: 24 obrazy/min. Kolor: 20 obrazy/min. | Spełnia Tak*/Nie* |
| 37. | Bezpieczne drukowanie | Tak | Spełnia Tak*/Nie* |
| 38. | Bezpieczne drukowanie z SSL | Tak | Spełnia Tak*/Nie* |
| 39. | Toner o dużej wydajności | do 8,000 stron | Spełnia Tak*/Nie* |
| 40. | Eksploatacja w zestawie | o wydajności do 2.000 stron | Spełnia Tak*/Nie* |
| 41. | Standardowy toner | o wydajności do 3,000 stron | Spełnia Tak*/Nie* |
| 42. | Materiały eksploatacyjne | Bęben do 50,000 stron A4 (3 strony na zadanie drukowania) | Spełnia Tak*/Nie* |
| 43. | Gwarancja | Minimum 12 m-cy – gwarancji | Pozycja podlegająca kryterium oceny ofert |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

## 4. Serwer plików typu NAS – 4 komplety

| LP | Nazwa komponentu | Wymagane parametry techniczne | Oferowane parametry techniczne |
|---|---|---|---|
| 1. | Cechy ogólne | Zakup wyspecjalizowanego serwera plików (Network Attached Storage - NAS), na którym będą przechowywane kopie zapasowe. Przechowywanie danych na takim urządzeniu zwiększa ich bezpieczeństwo z uwagi na zabezpieczenia sprzętowe (RAID) i programowe. | Producent:<br>……<br><br>Model:<br>……<br>Zamawiający wymaga dołączenia do oferty dokumentów:<br>Karta produktu |
| 2. | Procesor | Procesor uzyskujący w testach wydajnościowych publikowanych w serwisie https://www.cpubenchmark.net/ minimum 4580 pkt. | Model procesora:<br>……<br>Spełnia Tak*/Nie* |
| 3. | Obudowa | Tower o wymiarach minimum 166 mm x 343 mm x 243 mm (wysokość x szerokość x głębokość). | Spełnia Tak*/Nie* |
| 4. | Pamięć RAM | 8 GB pamięci SO-DIMM DDR4 ECC tego samego producenta co macierz. | Spełnia Tak*/Nie* |
| 5. | Ilość obsługiwanych dysków | Minimum 8 dysków o maksymalnej pojemności 16TB każdy, po podłączeniu modułów rozszerzających minimum 18 dysków. | Spełnia Tak*/Nie* |
| 6. | Zainstalowane dyski | 8 dysków o pojemności 4TB każdy zgodne z listą kompatybilności oferowanej macierzy oraz charakteryzujące się następującymi parametrami:<br>- prędkość obrotowa: minimum 5400 RPM,<br>- pamięć cache: minimum 256MB,<br>- gwarancja: minimum 36 miesięcy,<br>- MTBF: minimum 1 milion,<br>- usługa odzyskiwania danych. | Producent:<br>……<br>Model dysku:<br>……<br>Pojemność:<br>……<br><br>Spełnia Tak*/Nie* |
| 7. | Interfejsy sieciowe | 4 x Gigabit (10/100/1000); Wsparcie dla Link Agregation. Możliwość rozszerzenia o dodatkowe 2 porty 10Gb SFP+ / RJ-45. | Spełnia Tak*/Nie* |
| 8. | Porty | 4 x USB 3.2 1. Generacja 1, 2 x eSATA | Spełnia Tak*/Nie* |
| 9. | Wskaźniki LED | Status, HDD 1-8, zasilanie, LAN 1-4 | Spełnia Tak*/Nie* |
| 10. | Obsługa RAID | Basic, JBOD, RAID 0,1,5,6,10, SHR wraz z obsługą dysków typu hot spare. | Spełnia Tak*/Nie* |
| 11. | Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. | Spełnia Tak*/Nie* |
| 12. | Szyfrowanie | Możliwość szyfrowania wybranych udziałów sieciowych. | Spełnia Tak*/Nie* |
| 13. | Licencja na Kamery IP | W zestawie licencja na minimum dwie kamery z możliwością rozszerzenia do 40. | Spełnia Tak*/Nie* |
| 14. | Maks. liczba kamer IP | Obsługa do 40 kamer. | Spełnia Tak*/Nie* |
| 15. | Protokoły | SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP) | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| 16. | Usługi | Serwer VPN, Serwer pocztowy dla kilku domen, Stacja monitoringu, Integracja z Windows ADS, Firewall, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antyvirus, Klient VPN, Usługa DDNS, Zarządzanie przez komórkę, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki (min. 65 tys. w cały systemie), wirtualizacja, klaster HA z dwóch lub więcj urządzeń, backup Bare-Metal. | Spełnia Tak*/Nie* |
| 17. | Obsługa migawek | Maksymalna liczba migawek folderów współdzielonych: 1 024 | Spełnia Tak*/Nie* |
| 18. | Zarządzanie dyskami | SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów | Spełnia Tak*/Nie* |
| 19. | Język GUI | Polski | Spełnia Tak*/Nie* |
| 20. | Gwarancja i serwis | Minimum 12 m-cy gwarancji producenta | **Pozycja podlegająca kryterium oceny ofert** |
| 21. | Waga | Maksymalnie 6 kg | Spełnia Tak*/Nie* |
| 22. | Pobór mocy | Maksymalnie 60W w trybie pracy. Maksymalnie 27W w trybie hibernacja dysków. | Spełnia Tak*/Nie* |
| 23. | Certyfikaty | EAC, VCCI, CCC, RCM, KC, FCC, CE, BSMI | Spełnia Tak*/Nie* |
| 24. | System plików | Dyski wewnętrzne Btrfs lub EXT4. Dyski zewnętrzne Btrfs, FAT, NTFS, EXT3, EXT4, HFS+, exFAT | Spełnia Tak*/Nie* |
| 25. | Szyfrowanie | Mechanizm szyfrowania sprzętowego (AES-NI) | Spełnia Tak*/Nie* |
| 26. | Liczba wolumenów | Do 64 | Spełnia Tak*/Nie* |
| 27. | Liczba iSCSI Targetów | Do 128 | Spełnia Tak*/Nie* |
| 28. | Liczba iSCSI LUN | Do 256 | Spełnia Tak*/Nie* |
| 29. | Liczba kont użytkowników | Do 2048 | Spełnia Tak*/Nie* |
| 30. | Liczba grup | Do 256 | Spełnia Tak*/Nie* |
| 31. | Głośność pracy | Maksymalnie 24 dB(A) | Spełnia Tak*/Nie* |
| 32. | Zasilacz | Zasilacz wewnętrzny o mocy maksymalnie 250W | Spełnia Tak*/Nie* |
| 33. | Chłodzenie | Minimum 2 wentylatory o rozmiarze 120 mm x 120 mm | Spełnia Tak*/Nie* |
| 34. | Usługa backupu | 1. Zintegrowane rozwiązanie do tworzenia kopii zapasowych dla serwerów fizycznych z systemem Windows, komputerów, serwerów plików rsync/SMB oraz maszyn wirtualnych VMware vSphere/Microsoft Hyper-V.<br>2. Centralny interfejs zarządzania służący do monitorowania stanu wszystkich zadań tworzenia kopii zapasowych, zużycia pamięci masowej i transmisji danych historycznych.<br>3. Różne metody przywracania, w tym przywracanie całego urządzenia, natychmiastowe przywracanie, szczegółowe odzyskiwanie plików.<br>4. Maksymalna wydajność tworzenia kopii zapasowych i pamięci masowej dzięki zastosowaniu funkcji Changed Block Tracking (CBT), narzędzia RCT (Resident Change Tracking) oraz deduplikacji globalnej w miejscu składowania kopii zapasowych.<br>5. Elastyczne zasady planowania i przechowywania w celu dostosowywania strategii tworzenia kopii zapasowych.<br>6. Szczegółowe logi i raporty umożliwiające śledzenie stanów kopii zapasowych i diagnostykę problemów. | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

## 5. System do zarządzania infrastrukturą IT w siedzibie Zamawiającego – 70 licencji

| Lp. | Parametr | Wymagania minimalne | Oferowane parametry |
|---|---|---|---|
| 1. | Architektura / budowa | System musi umożliwić bezproblemową i stabilną obsługę co najmniej 2000 agentów jednocześnie. | Producent: ……<br>Nazwa i wersja oprogramowania: …… |
| | | System musi posiadać następującą architekturę: | |
| | | Agent – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej. | |
| | | Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych). | |
| | | Panel pracownika – aplikacja webowa dostępna dla pracowników i uruchamiana na komputerach pracowników udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach zgodnie ze specyfikacją opisaną poniżej. | |
| | | Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z agentami. | |
| | | Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej. | |
| | | Komponenty Agent, konsola administracyjna, serwer, baza danych muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerów aktualizacji producenta systemu. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja agentów musi przebiegać w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie ze strony producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją. | |
| | | System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, pakietów, pomoc i inne wbudowane bazy wiedzy. | |
| | | Agent do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI. | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | Agent musi być dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku msi. | |
| | | Agent musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej. | |
| | | System musi posiadać możliwość wygenerowania instalatora Agenta, który nie będzie wymagał uprawnień administracyjnych do zainstalowania. | |
| | | Agent musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa). | |
| | | System powinien umożliwiać generowanie unikatowego identyfikatora agenta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków. | |
| | | Agent musi mieć definiowalny priorytet pracy (ABOVE_NORMAL, NORMAL, BELOW_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów. | |
| | | Agent musi wspierać do sześciu różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu agenta. | |
| | | System musi umożliwiać komunikację pomiędzy agentami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem. | |
| | | System musi mieć możliwość współpracy komponentów agent i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami agentów. | |
| | | System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem realizujące co najmniej: usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nieprzyrostowe, zmniejszanie bazy danych. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartości parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie. System musi prezentować historię przeprowadzonych konserwacji/utrzymania. | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| 2. | Wymagania systemowe | Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, Firefox, Chrome, Opera). | |
| | | Agent musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa. | |
| | | Serwer musi działać na systemach 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11. | |
| | | Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2012/2012R2/2016/2019/2022, Windows 10) oraz Java 8 (JRE lub JDK), Apache Tomcat 8+. | |
| | | Baza danych musi działać na silniku Microsoft SQL Server 2012/2014/2016/2017/2019 w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition). | |
| | | System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare. | |
| | | Interfejsy | |
| | | System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie. | |
| | | Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID. | |
| | | Import z Active Directory musi wspierać obsługę protokołów SSL oraz TLS. | |
| | | Import z Active Directory musi umożliwiać podanie więcej niż jednej domeny. | |
| | | System musi umożliwiać import użytkowników z zewnętrznego pliku CSV. | |
| | | System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switche itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Interfejs dodatkowo musi umożliwiać importowanie użytkowników, struktur i licencji. Import musi umożliwiać pobieranie danych z dowolnego źródła danych o dowolnej strukturze danych z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane. | |
| | | System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS. | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| 3. | Funkcjonalność agenta | System musi umożliwiać pełne zdalne zarządzanie agentami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączania agenta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego), uruchamiania i wyłączania polityk w obszarze bezpieczeństwa (DLP). | |
| | | Agent musi mieć możliwość konfiguracji zakresu skanowania plików w oparciu o nazwę plików (z uwzględnieniem znaków wieloznacznych), lokalizację na konkretnym dysku, datę utworzenia pliku oraz wielkość. | |
| | | Agent musi mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej a konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkowniku, który go wyświetlił. | |
| | | Agent musi mieć budowę modułową – uniemożliwienie pracy jednego z modułów (np. w wyniku niekompatybilnego systemu operacyjnego, pracy programów firm trzecich, awarii sprzętowej) nie może blokować pracy całego Agenta. | |
| | | Po wykryciu nieprawidłowości w pracy dowolnego z modułów Agent powinien podjąć samoczynną próbę jego naprawy i przywrócenia do działania. | |
| | | Funkcjonalność konsoli administracyjnej. | |
| | | Konsola musi być w pełni polskojęzyczna oraz dodatkowo posiadać wersje językowe niemiecką oraz angielską. | |
| | | Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie). | |
| | | Konsola administracyjna musi posiadać dashboardy – dashboard użytkownika, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie. | |
| | | Dashboard użytkownika jest budowany samodzielnie przez użytkownika poprzez wybór szybkiego skrótu do dowolnego ekranu aplikacji lub wybór dowolnego widgetu. | |
| | | Dashboard prezentujący parametry sieci zawiera widgety pogrupowane w kategorie: Czat, Gry, Peer to peer, Streaming, Usługa podstawowa, Usługa podstawowa (szyfrowana), Złośliwe oprogramowanie. | |
| | | Dla każdej z usług prezentowane są relacje do wszystkich komputerów zawierające połączenia: powolne, nieosiągalne, rozłączone i poprawne wraz z czasami połączeń. | |
| | | Dashboard prezentujący informacje o bezpieczeństwie zawiera widgety zawierające informacje: błędy serwera zadań, błędy smart, komputery bez bitlockera, komputery bez połączenia z serwerem, komputery z błędami typu critical / error / warning, duży transfer sieciowy, komputery bez agenta, komputery offline, komputery online, komputery z naruszoną polityką dlp, komputery z nieaktualną polityką dlp, liczba administratorów lokalnych w systemie (online), logowanie w godzinach nocnych, monitorowanie transferu do dysków chmurowych, nieautoryzowana pamięć usb, nowe komputery, nowe urządzenia w sieci, oprogramowanie zabronione, przekroczone cal, przekroczone | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | licencje, subskrypcje, które wygasły, systemy bez wsparcia, wielokrotne logowanie, wysokie użycie cpu, wysokie użycie ram, zaległe szkolenia wideo, zaległe wiadomości elearning, zbyt mało miejsca na hdd, zmiany na kontach użytkowników, zmiany tcp/ip. | |
| | | Konsola administracyjna musi być wyposażona w panel zawierający graficzne widgety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi. | |
| | | Dane na widgetach muszą być aktualizowane automatycznie nie rzadziej niż 1 raz/ godzinę lub w każdym czasie na życzenia użytkownika. | |
| | | Widgety muszą być skojarzone dziedzinowo ze wszystkimi obszarami zarządzania infrastrukturą, a każdy obszar powinien być reprezentowany przez min. 5 widgetów (np. w obszarze zarządzania komputerami system powinien być wyposażony w widgety zawierające: ilość komputerów w ramach danego typu, ilość komputerów on/off-line, strukturę komputerów wg ilości pamięci RAM, ilość komputerów wg ilości wolnego miejsca na dysku, ilość komputerów wg dat ostatnich połączeń) | |
| | | Z każdego widgetu można uzyskać szczegółową informację analityczną (listę z danymi składającymi się na wybraną wartość na widgecie). | |
| | | Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja agenta, stanu agenta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera. | |
| | | Konsola musi umożliwić bezpośrednie przejście do witryny internetowej producenta z poziomu repozytorium producentów (o ile taka jest dostępna, np. DELL). | |
| | | Konsola musi umożliwić bezpośrednie przejście do strony producenta zawierającej dodatkowe dane konfiguracyjne na temat konkretnego komputera w oparciu o Service Tag lub inny unikatowy identyfikator (np. Dell) | |
| | | Konsola musi zawierać w sobie pełną dokumentację systemu, dokumentacja musi być na bieżąco aktualizowana poprzez automatyczne mechanizmy aktualizacji z serwera aktualizacji producenta. | |
| | | Funkcjonalność panelu pracownika | |
| | | Automatyczne uruchamianie panelu w momencie zalogowania użytkownika do systemu operacyjnego. | |
| | | Zakres informacji w panelu jest definiowany przez administratora w formie schematów przypisywanych dla wybranych grup pracowników. | |
| | | Panel pracownika użytkowany przez kierownika zawiera dodatkowo dane dostępne w panelach podległych pracowników w formie danych skumulowanych i analitycznych. | |
| | | Wszelkie informacje udostępniane w panelu pracownika pogrupowane są w logiczne sekcje, z możliwością indywidulanego bądź grupowego włączania / wyłączania (ukrywania) sekcji. | |
| | | Sekcje informacyjne panelu pracownika | |
| | | Zalogowany użytkownik – imię i nazwisko, IP, nazwa komputera, informacje z AD – nazwa domenowa, nr telefonu, nr telefonu komórkowego, stanowisko | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| 4. | Dashboard | Moje zgłoszenia – zgłoszenia do wsparcia technicznego (nowe, otwarte, rozwiązane). | Spełnia Tak*/Nie* |
| | | Mój komputer – wykorzystanie RAM, dysku, CPU. | |
| | | Produktywność – czas zalogowania, aktywność, produktywność. | |
| | | Baza wiedzy – najczęściej odwiedzane artykuły wsparcia technicznego. | |
| | | Szkolenia – lista filmów szkoleniowych do zapoznania przez pracownika. | |
| | | Wiadomości – lista ostatnich wiadomości przesłanych pracownikowi. | |
| 5. | Sprzęt | Komputery przypisane do pracownika (nr seryjny, MAC, IP, data ostatniego logowania). | Spełnia Tak*/Nie* |
| | | Komputery używane przez pracownika (nr seryjny, MAC, IP, data ostatniego logowania). | |
| | | Urządzenia przypisane przez pracownika (nr seryjny, typ, IP). | |
| | | Urządzenia używane przez pracownika (nr seryjny, typ, IP). | |
| | | Oprogramowanie | |
| | | Lista używanego oprogramowania (nazwa aplikacji, wersja, Producent, użycie w okresie ostatnich 3, 6, 12 miesięcy, data ostatniego uruchomienia). | |
| 6. | Zarządzanie licencjami | System musi umożliwiać zarządzanie licencjami w ramach dowolnego elementu struktury organizacyjnej (dla wybranej struktury organizacyjnej pokazuje liczbę instalacji i liczbę licencji w danym modelu licencjonowania wraz z listą komputerów). | Spełnia Tak*/Nie* |
| | | System musi dawać możliwość wykonywania (historia) wielu audytów legalności i zapamiętywać wyniki tych audytów w odniesieniu do systemów operacyjnych jak i aplikacji/pakietów, z uwzględnieniem segmentu struktury organizacyjnej. | |
| | | Zarządzanie oprogramowaniem musi następować z podziałem na aplikacje i pakiety oprogramowania. | |
| | | System musi pozwalać na zdefiniowanie dowolnej ilości tzw. „standardów oprogramowania", które definiują 3 kategorie oprogramowania: „oprogramowanie standardowe" – pozycje z tej listy są wymagane do zainstalowania obowiązkowo na każdym komputerze, „oprogramowanie dodatkowe" – pozycje z tej listy mogą być zainstalowane (nie jest to wymagane) a instalacja odbywa się na wniosek samego użytkownika lub jego przełożonego, „oprogramowanie nieokreślone" – oprogramowanie nie należące do żadnej z dwóch powyżej zdefiniowanych kategorii a zidentyfikowane na komputerze. | |
| | | System umożliwia zdefiniowanie listy aplikacji zabronionych. | |
| | | System umożliwia utworzenie schematów (kolekcji) oprogramowania zabronionego i w momencie pojawienia się ich na komputerze przystępuje do automatycznego odinstalowania w trybie cichym (bez interfejsu). | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | System musi umożliwiać zdefiniowanie dowolnej kategorii oprogramowania/pliku/procesu i samodzielnej przydzielenie oprogramowania/pliku/procesu do kategorii. | |
| | | W oparciu o Machine learning system umożliwia analizę procesów oraz przypisanie im odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem uruchamianych procesów. | |
| | | Automatyczne przypisanie kategorii do każdego uruchomionego procesu. | |
| | | Niezależność od zewnętrznych dostawców bazy wzorców procesów. | |
| | | System zbiera szczegółowe informacje o systemie operacyjnym (wersja, edycja, service pack, poprawki, data instalacji). | |
| | | System umożliwia odczytywanie identyfikatorów i kluczy produktowych dla systemu operacyjnego oraz dowolnego oprogramowania, tam gdzie jest to tylko technicznie możliwe. | |
| | | System wspiera następujące typy licencji: Enterprise, Licensed concurrent, Licensed Name, Licensed per Processor, Licensed per Seat, Licensed per Server, OEM, OEM Downgrade, Open, Select, MOLP Open Value (Company wide), MOLP Open Value (non-Company wide), MOLP Open Value Subscription, CAL, SAAS, Trial, Shareware, Cal Per User. | |
| | | System automatycznie klasyfikuje i rozlicza licencje OEM dla systemów operacyjnych oraz licencje typu freeware dla aplikacji. | |
| | | System musi pomijać w rozliczeniu licencje wygasłe (po terminie ważności) i informować administratora o wygasaniu licencji. | |
| | | System musi umożliwiać wyróżnianie licencji zabezpieczonych kluczami sprzętowymi. | |
| | | System automatycznie wskazuje liczbę posiadanych licencji oraz liczbę używanego oprogramowania (pokazuje braki oraz nadwyżki). | |
| | | System automatycznie uwzględnia i rozlicza licencje typu Upgrade i Downgrade wg zdefiniowanych przez użytkownika reguł. | |
| | | System prezentuje datę instalacji oprogramowania. | |
| | | System umożliwia ewidencję licencji (data zakupu, cena, dostawca, nr faktury, typ licencji, klucz produktowy, identyfikator produktowy, data wygaśnięcia, nr dokumentu OT, nr zapotrzebowania) poprzez rejestrację dokumentów źródłowych (faktur zakupu) z możliwością dołączenia dowolnych załączników z repozytorium. | |
| | | System umożliwia przypisanie licencji do użytkownika i/lub komputera oraz udostępnia informację o licencjach zarejestrowanych i jednocześnie wolnych (nieprzypisanych). | |
| | | System umożliwiać zbieranie informacji na temat uruchamianych aplikacji na inwentaryzowanych komputerach (m.in. czas uruchomienia, nazwa zalogowanego użytkownika, nazwa aplikacji). System musi posiadać mechanizm zabezpieczający przed powstaniem niekompletnych lub niewłaściwych zapisów w wyniku braku zasilania lub innych awarii inwentaryzowanego systemu/sprzętu). | |
| | | System musi udostępniać informację o uruchamianych aplikacjach w okresie 3/6/12 miesięcy oraz udostępniać datę ostatniego uruchomienia. | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | System musi automatycznie wyliczać przybliżone oszczędności z zakupionych a nie zainstalowanych aplikacji, przybliżone oszczędności z zainstalowanych a niewykorzystanych licencji oraz przybliżone nakłady konieczne na uzyskanie pełnej legalności. | |
| | | System musi umożliwiać podgląd historii zmian aplikacji i pakietów na komputerach. | |
| | | System musi umożliwiać zdalne odinstalowanie oprogramowania na jednym bądź wybranych komputerach. | |
| | | System musi udostępniać informacje o stopniu wykorzystania aplikacji / pakietów dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie czasu. W/w informacja winna być przedstawiona również w postaci graficznej. | |
| | | System musi udostępniać informacje o stopniu wykorzystania oprogramowania typu web dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie czasu. W/w informacja winna być przedstawiona również w postaci graficznej. | |
| 7. | Inwentaryzacja sprzętu komputerowego | System musi umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem). | Spełnia Tak*/Nie* |
| | | System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language. | |
| | | System ma umożliwiać skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu). | |
| | | System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania. | |
| | | System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza począwszy od wskazanego miejsca w hierarchii kluczy rejestru. | |
| | | System ma umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu). | |
| | | System ma umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART). | |
| | | System musi umożliwić budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku. | |
| | | System musi umożliwiać skanowanie uprawnień użytkowników oraz grup użytkowników wraz z informacją o uprawnieniach, czy konto jest włączone, zablokowane, czy wymagana jest zmiana hasła, czy hasło wygasa, czy hasło jest wymagane). | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu. | |
| | | System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent). | |
| | | System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne. | |
| | | System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów. | |
| | | System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik). | |
| | | System umożliwia dodawanie notatek do każdej pozycji sprzętu. | |
| | | System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części). | |
| | | System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium. | |
| | | System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkowania, likwidacja). | |
| | | Inwentaryzacja urządzeń podłączanych do komputera | |
| | | System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.). | |
| | | System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika. | |
| | | System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika). | |
| | | System musi mieć możliwość przypominania o upływającym terminie gwarancji. | |
| | | System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium wewnętrznego systemu. | |
| | | System udostępnia informację o wartości wprowadzonego sprzętu. | |
| | | System musi umożliwiać samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów oraz zapewniać automatyczną numerację tych dokumentów zapewniającą unikatowość. | |
| | | System musi pozwalać na kopiowanie (duplikację) dowolnego urządzenia dowolną ilość razy. | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | System musi pozwalać na ewidencję umów utrzymaniowych (SLA) w odniesieniu do zaewidencjonowanych licencji oraz urządzeń w zakresie co najmniej: nazwa, okres, data dokumentu, numer dokumentu, dostawca, osoba kontaktowa, wartość, opis, warunki oraz umożliwiać dołączenie dowolnej ilości załączników z repozytorium i powiązanie umowy utrzymaniowej z dowolną ilością zasobów (urządzenia, licencje). | |
| 8. | Zdalna administracja komputerami | System ma automatyczne wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika. | Spełnia Tak*/Nie* |
| | | System musi posiadać wbudowany skaner wyposażony w harmonogram skanowania umożliwiający wykrywanie (rozpoznawanie) komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro. | |
| | | System musi umożliwiać zarządzanie komputerami z technologią Intel vPro, w tym: Serial Over LAN, zdalne włączanie, wyłączanie komputera, zdalna konfiguracja BIOS, uruchomienie zdalnie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji. | |
| | | System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym (od VPro v.6). | |
| | | System musi umożliwiać za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacja oprogramowania, poprawek i aktualizacji (service pack, patch). | |
| | | System umożliwia zdalne podłączenie do wielu komputerów jednocześnie i podgląd oraz operowanie na pulpitach tych komputerów w technologii Ultra VNC. | |
| | | System musi umożliwiać uruchomienie do 6 sesji Ultra VNC na jednym ekranie. | |
| | | System musi umożliwiać uruchomienie sesji Ultra VNC w trybie podłączenia się do obecnie zalogowanego użytkownika oraz w trybie RDP (wylogowania użytkownika i przejęcia dostępu). | |
| | | System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania. | |
| | | Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego. | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status). | |
| | | System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, windows powershell. System posiada co najmniej 70 predefiniowanych poleceń. | |
| | | System musi umożliwiać zdalne połączenia do wielu komputerów jednocześnie, podgląd i operowanie na pulpitach tych komputerów w technologii WEBRTC. | |
| | | System musi umożliwiać za pomocą technologii WEBRTC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalację oprogramowania, poprawek i aktualizacji (service pack, patch). | |
| | | System musi umożliwiać poprzez technologię WEBRTC zdalne zarządzanie plikami (tworzenie, kopiowanie, usuwanie, przesyłanie) i wykorzystanie wiersza poleceń (cmd) oraz powershell bez konieczności podłączenia do komputera. | |
| | | System musi umożliwiać nagrywanie sesji połączeń WEBRTC jak i nawiązywanie komunikacji z użytkownikiem podczas sesji (czat). | |
| | | System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia. | |
| | | System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu. | |
| 9. | Automatyzacja | System ma mieć możliwość ustalania harmonogramu, zgodnie z którym uruchamiane są czynności konserwacyjne, naprawcze, porządkujące. | Spełnia Tak*/Nie* |
| | | Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania danej czynności (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartości parametrów wejściowych, a także zatrzymania/uruchomienia harmonogramu uruchomienia dla każdej z czynności. | |
| | | System musi mieć możliwość definiowania czynności wykonywanych automatycznie. | |
| | | System musi być wyposażony w następujące mechanizmy automatyzacji: wykonywanie kopii bezpieczeństwa bazy danych, identyfikacja aplikacji i pakietów, porządkowanie bazy danych / odbudowa indeksów, usuwanie nadmiarowych danych w bazie danych, usuwanie zewnętrznych plików (logów). | |
| | | System musi być wyposażony w mechanizmy informowania - wysyłania komunikatów (alerty) o: zasobach zakazanych (pliki erotyczne i pornograficzne), zasobach multimedialnych (pliki multimedialne), nowych komputerach w bazie danych, braku skanowania komputerów, brakach w licencjach, niewłaściwych datach systemowych komputerów, urządzeniach bez użytkowników, zdublowanych systemach operacyjnych, zakazanych procesach/stronach www /aplikacjach, wygasaniu serwisu lub licencji, przekroczeniu wielkości bazy danych, nadmiernym obciążeniu dysków twardych, nadmiernym obciążeniu sieci, nadmiernym obciążeniu sieci na komputerze, nadmiernym obciążeniu procesora, nadmiernym obciążeniu pamięci RAM, małej ilości wolnego miejsca na dysku, upływającej gwarancji. | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.). | |
| | | System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako). | |
| | | System musi umożliwiać tworzenie zadań cyklicznych dla komputerów. | |
| | | Obsługa zadań cyklicznych musi następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia, pierwszy/drugi/trzeci/czwarty/ostatni poniedziałek/wtorek/środa/czwartek/piątek/sobota/niedziela/dzień wolny/dzień powszedni co n miesięcy, nowe zadanie n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu, w pierwszy/drugi/trzeci/czwarty/ostatni, w dowolny dzień tygodnia, dzień wolny/dzień powszedni wybranego miesiąca, nowe zadanie n lat od wykonania. | |
| | | System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie. | |
| 10. | Zarządzanie magazynem IT | System musi umożliwiać obsługę magazynu IT. | Spełnia Tak*/Nie* |
| | | System musi umożliwiać obsługę dowolnej ilości magazynów w różnych lokalizacjach. | |
| | | System musi umożliwiać obsługę dokumentów PZ, WZ, MM+, MM-, LI. | |
| | | System musi prowadzić ewidencję materiałów w magazynach w oparciu o metodę FIFO (pierwsze przyszło pierwsze wyszło). | |
| | | System musi umożliwiać obsługę kodów kreskowych dla materiałów w magazynach. | |
| | | System musi udostępniać informację o wartościach materiałów w poszczególnych magazynach, stanach materiałów w magazynach, dokumentach dotyczących danego materiału w dowolnym magazynie. | |
| 11. | Repozytorium | Konsola administracyjna musi być wyposażona w repozytorium dokumentów dowolnego typu. | Spełnia Tak*/Nie* |
| | | Repozytorium musi umożliwiać: dodawanie nowych dokumentów dowolnego typu, przeszukiwanie, oznaczanie dokumentów (znaczniki TAG) więcej niż jednym znacznikiem, podgląd dokumentów, dołączanie dokumentów z repozytorium w dowolnym miejscu systemu, uzyskanie informacji w jakich miejscach systemu dany dokument repozytorium występuje. | |
| | | Kody kreskowe | |
| | | System wspiera obsługę kodów kreskowych jedno i dwuwymiarowych. | |
| | | System wspiera parametryzację kodu w zakresie wielkości graficznej kodu. | |
| | | System pozwala w każdym momencie na zmianę typu i atrybutów kodu. | |
| | | System informuje o błędzie generacji kodu, np. na skutek niewłaściwej długości wprowadzonego ciągu znaków w stosunku do danego standardu kodu. | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | Istnieje możliwość podglądu kodu oraz jednostkowego i masowego wydruku kodu / kodów. | |
| | | System musi generować kody kreskowe (jedno i dwuwymiarowe) dla każdego zaewidencjonowanego urządzenia w standardzie wybranym przez użytkownika: aztec, codabar, code128, code39, dataMatrix, EAN128, EAN13, EAN8, interleaved2of5, ITF14, PDF417, POSTNET, qrcode, royalMailCBC, UPCA, UPCE, USPSIntelligentMail. | |
| | | Obsługa kodów kreskowych nie może wymagać instalacji czcionek. | |
| | | Parametry kodu kreskowego (wymiary, wielkość i typ czcionki) muszą być definiowalne. | |
| | | System musi umożliwiać współpracę z zewnętrznymi czytnikami kodów. | |
| | | Monitorowanie drukarek sieciowych i wydruków | |
| | | System musi posiadać możliwość ewidencji wszystkich generowanych wydruków niezależnie od miejsca ich generowania oraz typu drukarki (lokalna, sieciowa). | |
| | | Ewidencja wydruków musi obejmować: nazwę i wielkość dokumentu, datę i godzinę wydruku, nazwę użytkownika drukującego, IP i nazwę komputera z którego dokonano wydruku, format dokumentu, informację i jedno bądź dwustronnym wydruku, informację o wydruku mono/kolor. | |
| | | System dla każdego wydruku, dla każdej drukarki musi obliczać rzeczywisty koszt wydruku w oparciu o wbudowany cennik wydruków obejmujący cenę papieru (w zależności od formatu) oraz cenę materiałów eksploatacyjnych (toner, tusz) dla danej drukarki, typu wydruku, rozmiaru papieru. | |
| | | System musi generować zestawienia pozwalające ustalić miejsca powstawania kosztów wydruków (komórki organizacyjne, użytkownicy) oraz stopień obciążenia poszczególnych urządzeń drukujących. | |
| | | System musi prognozować ilość i koszt wydruków na wszystkich drukarkach w okresie kolejnych 3,6,12 miesięcy. | |
| | | System musi pozwalać na grupowanie (kojarzenie) drukarek wg sterowników. | |
| | | Dla każdej z drukarek SNMP system musi udostępniać informacje: nr seryjny, IP, MAC, bieżący status drukarki, całkowitą ilość wydrukowanych stron, ilość wydrukowanych stron od uruchomienia, błędy, alerty, dostępne porty, stan pokryw, interfejsów sieciowych, rodzaj i ilości pamięci całkowitej i wykorzystanej, informacje o poziomie materiałów eksploatacyjnych | |
| 12. | Monitorowanie stron www | System musi posiadać możliwość monitorowania odwiedzanych stron www niezależnie od typu używanej przeglądarki internetowej. | Spełnia Tak*/Nie* |
| | | Ewidencja otwieranych stron musi dotyczyć wielu jednocześnie otwartych zakładek. | |
| | | Ewidencja otwieranych stron musi działać również, gdy otwierana jest strona z połączeniem szyfrowanym (https). | |
| | | Ewidencja musi obejmować co najmniej: nazwę i adres IP komputera, nazwę użytkownika, datę i godzinę, adres strony, łączny czas korzystania, czas aktywności, czas pasywności. | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | W oparciu o algorytmy sztucznej inteligencji - machine learning oraz deep learning system umożliwia analizę treści rtcstron www oraz przypisanie im – w oparciu o treść – odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem odwiedzanych stron. | |
| | | Każda odwiedzona strona otrzymuje atrybuty: czy SSL, czy jest bezpieczna, czy zawiera przekierowania, czy znajduje się na liście CERT, czy znajduje się na liście stron hazardowych, czy kategoria strony jest bezpieczna, czy jest produktywna. | |
| | | Monitorowanie serwerów WWW | |
| | | System musi umożliwiać monitorowanie wybranych serwerów www. | |
| | | System musi przedstawiać informację o działaniu wybranych serwerów oraz ich aktywności. | |
| | | System musi posiadać możliwość weryfikacji treści (tekstu) dostępnego na monitorowanej stronie. | |
| | | System w sposób graficzny musi przedstawiać działanie serwerów WWW wraz z wyszczególnieniem informacji dla każdego wybranego serwera (status, bieżący czas odpowiedzi, średni czas odpowiedzi za ostatnie 12 miesięcy, aktywność za ostatnie 3, 6, 12 miesięcy). | |
| 13. | Monitorowanie dziennika zdarzeń | System musi posiadać możliwość monitorowania dziennika zdarzeń wszystkich komputerów. | |
| | | Ewidencja zdarzeń musi następować w oparciu o definiowalną kategorię zdarzenia: critical, error, warning, info, audit failure, audit success, debug oraz typ dziennika: aplikacja, bezpieczeństwo, system. | |
| | | System musi pozwalać na zdefiniowanie ewidencji zdarzeń z komputerów na podstawie kategorii zdarzenia. | |
| | | Ewidencja musi zawierać: datę i godzinę zdarzenia, nazwę i adres IP komputera, typ zdarzenia, opis zdarzenia. | |
| | | System musi umożliwiać monitorowanie komunikatów Syslog. | |
| 14. | Monitorowanie pracy komputerów | System musi posiadać możliwość monitorowania daty włączenia i wyłączenia komputera niezależnie czy znajduje się w sieci lokalnej czy też poza nią i prezentować czas pracy komputera w układzie graficznym. | Spełnia Tak*/Nie* |
| | | System musi posiadać ewidencję daty i godziny przyłączenia i odłączenia komputera od systemu monitorującego. | |
| | | System musi ewidencjonować zdarzenia związane z logowaniem się użytkowników do danego komputera, również w przypadku podłączania się wielu użytkowników jednocześnie. | |
| | | Monitorowanie sesji zdalnych połączeń | |
| | | System musi prowadzić ewidencję sesji zdalnych połączeń na każdym komputerze. | |
| | | Informacja o nawiązanej sesji musi zawierać co najmniej: nazwę i adres IP komputera z którego nastąpiło połączenia, nazwę użytkownika nawiązującego połączenie, nazwę i adres IP komputera docelowego, adres portu połączenia. | |
| 15. | Raportowanie i eksport danych | Systemu musi umożliwiać wyeksportowania wybranych lub wszystkich danych do formatu xls, csv, OpenOffice calc, html, mht, xml, jpeg, png, gif, bmp. | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | System musi mieć możliwość kategoryzowania raportów (spośród wszystkich raportów) oraz dodawania raportów użytkownika (zaprojektowanych przez użytkownika). | |
| | | System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów. | |
| | | Generowanie raportu musi odbywać się po stronie serwera a nie klienta. | |
| | | System musi umożliwiać wieloinstancyjność raportowania (wiele otwartych raportów jednocześnie z wielu widoków). | |
| | | System musi mieć możliwość generowania i wyświetlania dowolnych wieloparametrycznych raportów w standardzie SAP Crystal Reports (rpt). | |
| | | System musi umożliwiać eksport danych z raportu do formatów: RPT, PDF, XLS, DOC, RTF. | |
| | | System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu). | |
| | | System musi posiadać co najmniej 150 zdefiniowanych raportów dotyczących wszystkich obszarów funkcjonalnych. | |
| | | Raporty z zakresu komputerów , Komputery – Karta graficzna – Procesor, Komputery – Serwery wg systemu operacyjnego, Komputery wg procesora – Skrócony, Komputery wg procesora – Wszystkie, Komputery wg producenta – Wszyscy Komputery wg struktur organizacyjnych – Skrócony Komputery wg struktury organizacyjnej – Wszystkie Komputery wg systemów operacyjnych – Skrócony Komputery wg systemów operacyjnych – Wszystkie Komputery wg typu – Desktop, Komputery wg typu – Hyper-V, Komputery wg typu – Mobile Komputery wg typu – Nieokreślone, Komputery wg typu – Server, Komputery wg typu – Virtual Machine, Komputery wg typu – VMWare, Komputery wg typu – Wszystkie typy, Zestawienie komputerów wg typu – Skrócony, Komputery online, Komputery niezautoryzowane, Komputery offline Komputery, online Komputery w magazynie, Komputery w naprawie, Komputery wszystkie, Komputery wycofane, Komputery zablokowane, Komputery zautoryzowane Komputery zlikwidowane, Komputery z Intel Anti-Theft, Komputery z Intel VPro, Raporty z zakresu wirtualizacji Wirtualizacja – Maszyny wirtualne, Wirtualizacja – Serwery wirtualizacji, Wirtualizacja Raporty z zakresu urządzeń Urządzenia – Notatki, Urządzenia – USB – Dodane, Urządzenia – USB – Wykryte, Urządzenia – USB – Wszystkie, Urządzenia – USB – Biała lista, Urządzenia – Serwis, Urządzenia – Inwentaryzacja – Kody kreskowe, Urządzenia – Inwentaryzacja, Urządzenia – Inwentaryzacja – Porównanie inwentaryzacji, Urządzenia – Utrzymanie Urządzenia, Raporty z zakresu sieci. | |
| | | z wykorzystaniem imiennego konta administratorów aplikacji i hasła, | |
| | | za pośrednictwem jednokrotnego uwierzytelniania poprzez Active Directory, | |
| | | za pośrednictwem jednokrotnego uwierzytelniania poprzez CAS, | |
| | | za pomocą kluczy uwierzytelniających. | |
| | | Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej. | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków). | |
| | | Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport. | |
| | | System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie. | |
| | | Uwierzytelnianie za pomocą kluczy | |
| | | Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe wraz z hasłem, które umożliwia jednoczesną pracę wielu użytkownikom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory/LDAP. | |
| | | Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania w oparciu o RSA 512/1024/RSA 2048 bit, ECDSA 192/256 bit, DES/3DES, AES 128/192/256 bit, SHA-1 / SHA-256. | |
| | | Wykorzystywane klucze muszą posiadać wsparcie dla systemów Windows 7/8.1/10 i Windows Server 2012/2016/2019. | |
| | | System musi udostępniać historię korzystania z poszczególnych opcji przez wybranych użytkowników/administratorów. | |
| | | System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy agentami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera. | |
| | | System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nieprzyrostowej oraz udostępniać informacje o rezultacie wykonania kopii. | |
| | | System musi pobierać dane z widoków (view) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych. | |
| | | W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy). | |
| | | System musi być wyposażony w mechanizmy powtórnego załadowania danych historycznych pochodzących od agentów. | |
| | | Pełne logowanie błędów w celu weryfikowania nieprawidłowości. | |
| | | Przechowywanie logów systemowych. | |
| | | Przechowywanie logów bezpieczeństwa. | |
| | | Przechowywanie logów aktywności użytkowników i administratorów. | |
| | | Pobieranie logów z agentów z poziomu konsoli administracyjnej. | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | Możliwość eksportu logów. | |
| | | Definiowanie maksymalnego czasu przechowywania plików log. | |
| | | System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji. | |
| | | Wsparcie i pomoc | |
| | | System musi posiadać dokumentację w postaci min. 20 filmów instruktażowych/nagrań z webinarów w języku polskim. | |
| | | System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim. | |
| | | Pomoc techniczna musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00. | |
| 16. | Gwarancja | Gwarancja minimum 12 m-cy | |
| 17. | Wdrożenie | 1. Wdrożenie realizowane jest bezpośrednio przez wykwalifikowane wsparcie Producenta oprogramowania,<br>2. Wdrożenie realizowane jest w formie zdalnej,<br>3. Komunikacja musi odbywać się w języku polskim,<br>4. Wdrożenie obejmuje pełną konfigurację wszystkich modułów niezbędnych do uruchomienia systemu ,<br>5. Wdrożenie zakończone jest szkoleniem z obsługi oprogramowania zakończone certyfikatem dla administratora systemu wystawionym bezpośrednio przez producenta oprogramowania Wykonawca przedłoży do oferty dokument poświadczony przez Producenta o przeprowadzeniu wdrożenia przez osoby posiadające autoryzacje Producenta . | Spełnia Tak*/Nie*<br><br>Zamawiający wymaga dołączenia do oferty dokumentów:<br>Dokument poświadczony przez Producenta o przeprowadzeniu wdrożenia przez osoby posiadające autoryzację Producenta |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

## 6. Urządzenia typu UPS dla stacji roboczych – 43 szt.

| Lp. | Nazwa komponentu | Wymagane parametry techniczne | Oferowane parametry techniczne |
|---|---|---|---|
| 1. | Przeznaczenie urządzenia | Urządzenie przeznaczone do pracy ze stacją roboczą użytkownika, zabezpieczenie pracy w przypadku zaniku prądu. | Producent: ……<br>Model i wersja:<br>……<br><br>Zamawiający wymaga dołączenia do oferty dokumentów:<br>Karta produktu |
| 2. | Topologia | Line-interactive | Spełnia Tak*/Nie* |
| 3. | Moc pozorna | Nie mniej 950 VA | Spełnia Tak*/Nie* |
| 4. | Moc skuteczna | Nie mniej 520 W | Spełnia Tak*/Nie* |
| 5. | Napięcie wejściowe | 140 - 300 V | Spełnia Tak*/Nie* |
| 6. | Kształt napięcia wyjściowego | Sinusoida schodkowa | Spełnia Tak*/Nie* |
| 7. | Gniazda wyjściowe | RJ-45 (in/out) , French/Belgian – minimum 4 szt. | Spełnia Tak*/Nie* |
| 8. | Czas przełączania | Nie więcej niż 6 ms | Spełnia Tak*/Nie* |
| 9. | Czas podtrzymania dla obciążenia 50% | Nie mniej niż 6,5 min | Spełnia Tak*/Nie* |
| 10. | Czas podtrzymania dla obciążenia 100% | Nie mniej niż 1 min | Spełnia Tak*/Nie* |
| 11. | Średni czas ładowania | Nie więcej niż 8 h | Spełnia Tak*/Nie* |
| 12. | Interfejs komunikacyjny | USB | Spełnia Tak*/Nie* |
| 13. | Zabezpieczenia | Przeciwprzepięciowe | Spełnia Tak*/Nie* |
| 14. | Sygnalizacja pracy | Diody LED, Dźwiękowa | Spełnia Tak*/Nie* |
| 15. | Typ obudowy | Tower | Spełnia Tak*/Nie* |
| 16. | Zabezpieczenia | Zabezpieczenie linii LAN (RJ45) , Automatyczna regulacja napięcia (AVR) | Spełnia Tak*/Nie* |
| 17. | Wysokość/Szerokość/Głębokość | 160 mm /120 mm / 355 mm | Spełnia Tak*/Nie* |
| 18. | Waga | Nie więcej niż 6,1 kg | Spełnia Tak*/Nie* |
| 19. | Gwarancja | Nie mniej 24 miesiące (gwarancja producenta) | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

## 7. Sprzętowy firewall typu UTM – 1 szt.

| Lp. | Nazwa komponentu | Wymagane parametry techniczne | Oferowane parametry techniczne |
|---|---|---|---|
| 1. | Wymagania Ogólne | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.<br>System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.<br>W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.<br>System musi wspierać IPv4 oraz IPv6 w zakresie:<br>• Firewall,<br>• Ochrony w warstwie aplikacji,<br>• Protokołów routingu dynamicznego. | Producent:<br>……<br>Model i wersja:<br>……<br><br>Zamawiający wymaga dołączenia do oferty dokumentów:<br>Karta produktu |
| 2. | Redundancja, monitoring i wykrywanie awarii | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.<br>2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.<br>3. Monitoring stanu realizowanych połączeń VPN.<br>4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. | Spełnia Tak*/Nie* |
| 3. | Interfejsy, Dysk, Zasilanie: | 1. System realizujący funkcję Firewall musi dysponować minimum:<br>• 10 portami Gigabit Ethernet RJ-45.<br>• 2 gniazdami SFP 1 Gbps.<br>2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.<br>3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.<br>4. System musi być wyposażony w zasilanie AC. | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| 4. | Parametry wydajnościowe: | 1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.<br>2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.<br>3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. | Spełnia Tak*/Nie* |
| 5. | Ochrona przed malware | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).<br>2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.<br>3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).<br>4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.<br>5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.<br>6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. | Spełnia Tak*/Nie* |
| 6. | Ochrona przed atakami | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.<br>2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.<br>3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.<br>4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.<br>5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.<br>6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.<br>7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. | Spełnia Tak*/Nie* |
| 7. | Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.<br>2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.<br>3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.<br>4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.<br>5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| 8. | Kontrola WWW | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.<br>2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.<br>3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.<br>4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.<br>5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.<br>6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.<br>7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. | Spełnia Tak*/Nie* |
| 9. | Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:<br>• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.<br>• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.<br>• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.<br>2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.<br>3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.<br>4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. | Spełnia Tak*/Nie* |
| 10. | Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.<br>2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.<br>3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.<br>4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.<br>5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.<br>6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. | |
| 11. | Logowanie | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.<br>2. W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku.<br>3. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.<br>4. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.<br>5. Musi istnieć możliwość logowania do serwera SYSLOG. | Spełnia Tak*/Nie* |
| 12. | Certyfikaty | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:<br>• ICSA lub EAL4 dla funkcji Firewall. | Spełnia Tak*/Nie* |
| 13. | Serwisy | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:<br>a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [12] miesięcy.<br>b) usługa realizowana w chmurze na okres [12] miesięcy umożliwiająca logowanie i raportowanie z czasem retencji logów minimum 1 rok. | Spełnia Tak*/Nie* |
| 14. | Gwarancja oraz wsparcie | 1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min. 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24hx7dni. | **Pozycja podlegająca kryterium oceny ofert** |
| 15. | Rozszerzone wsparcie serwisowe | Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym w przypadku awarii wymianę sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wymaganej gwarancji.<br>Do zamawianego sprzętu Wykonawca zapewni usługę wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Partnera Serwisowego Producenta świadczona w języku polskim w zakresie<br>• wsparcie telefoniczne zespołu certyfikowanych inżynierów<br>• pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu<br>• doradztwo w zakresie konfiguracji<br>• zdalne wsparcie techniczne | **Pozycja podlegająca kryterium oceny ofert**<br><br>Spełnia Tak*/Nie*<br><br>Zamawiający wymaga dołączenia do oferty dokumentów:<br>Dokument potwierdzający gotowość świadczenia wsparcia technicznego |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | • pomoc w zakładaniu zgłoszeń serwisowych u producenta<br>• pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą)<br>• przygotowanie urządzenia do zdalnej konfiguracji<br>• zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika<br>• minimum 10 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika<br>Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji winien być nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.<br>Do oferty należy załączyć dokument wystawiony przez Producenta lub Autoryzowanego Dystrybutora potwierdzający gotowość świadczenia usługi serwisu wraz z certyfikatem ISO 9001 | w języku polskim na rzecz Zamawiającego i wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej<br>Certyfikat ISO 9001 podmiotu serwisującego |
| 16. | Kontrola dostępu | System do kontroli dostępu musi charakteryzować się następującymi cechami:<br>a. Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor).<br>b. System musi odsługiwać minimum 70 urządzeń klienckich (w tym gości). Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniania po rozłączeniu urządzenia.<br>c. Praca jako maszyna wirtualna.<br>d. Musi posiadać wbudowany serwer Radius oraz TACACS +<br>e. Musi wspierać RADIUS VSA co najmniej 100 producentów, w tym:<br>o Cisco Systems<br>o Fortinet<br>o Microsoft<br>o Alcatel-lucent Enterprise<br>o Aruba Networks<br>o Huawei<br>o Extreme Networks<br>o PaloAlto<br>f. System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera.<br>g. System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego.<br>h. Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.<br>i. Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych<br>o Microsoft Active Directory<br>o Radius<br>o Kerberos | Producent:<br>……<br>Podać nazwę pakietu licencji:<br>……<br><br>Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | o LDAP<br>o ODBC<br>o Współpraca z serwerami tokenów<br>j. Musi obsługiwać metody profilowania<br>o DHCP<br>o TCP<br>o MAC OUI<br>o SNMP<br>o Cisco device sensor<br>k. Wspierać protokoły<br>o Radius, Radius CoA, TACACS +, web authentication, SAML v2.0<br>o EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)<br>o PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD)<br>o TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)<br>o EAP-TLS<br>o PAP, CHAP, MSCHAPv1 i v2, EAP-MD5<br>o NAC, Microsoft NAP<br>o Windows machine authentication<br>o MAC Auth<br>o Audit (role oparte na porcie oraz skanowanie podatności)<br>o OCSP (Online Certificate Status Protocol)<br>o SNMP generic MIB, SNMP private MIB<br>o CEF (Common Event Format), LEEF (Log Event Extended Format)<br>o TLS 1.2<br>l. Funkcja integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami.<br>m. Maszyna wirtualna musi mieć możliwość uruchomienia na platformach witalizacyjnych:<br>o Co najmniej ESX 4.0, ESXi 4.1 do 6.0<br>o Co najmniej Hyper-V 2012 R2 oraz Windows 2012 R2 enterprise<br>n. Posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (5500). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte.<br>System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności:<br>o Samodzielna rejestracja klientów gościnnych w oparciu o:<br>o Adres e-mail<br>o Numer telefonu (wiadomość SMS)<br>o Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdący się w wiadomości link) | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | o Logowanie w oparciu o portale społecznościowe<br>o Funkcja integracji z systemami trzecimi poprzez API<br>o Wsparcie dla tworzenia komercyjnych systemów HOT-SPOT wykorzystujących do płatności systemy płatności karta kredytową<br>o Wbudowany system reklamowy umożliwiający integrację z zewnętrznymi serwisami umożliwiającymi w prosty sposób promowanie ofert promocyjnych, materiałów multimedialnych oraz aplikacji mobilnych.<br>o Wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych.<br>o Funkcja personalizacji strony gościnnej<br>• Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.<br>• Konfiguracja urządzeń ma odbywać się bez potrzeby angażowania pracowników działo IT<br>• System musi wspierać obsługę następujących systemów operacyjnych<br>o MS Windows<br>o Mac OS X<br>o iOS<br>o Android<br>o Chromebook<br>o Ubuntu<br>• Umożliwienie klientowi samo rejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci<br>• Automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej<br>• Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu.<br>• Funkcja tworzenia unikalnych certyfikatów dla urządzeń.<br>• Wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń<br>• Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID<br>• Posiadać moduł odpowiedzialny za kontrolę końcówek klienckich. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.<br>System kontroli końcówek klienckich musi mieć następujące funkcjonalności:<br>• System musi wspierać następujące systemy operacyjne<br>o Microsoft Windows 7 i nowsze (może być uruchomiony jako serwis)<br>o Apple Mac OS X 10.7 i nowsze<br>o Red HAT Enterprise Linux 4 i nowsze<br>o CentOS 4 (Community Enterprise Operating System) i nowsze<br>o Fedora Core 5 i nowsze<br>o SUSE linux 10.x i nowsze<br>• Funkcja kontroli stanu oprogramowania anty-wirusowego, anty-spyware, firewall<br>• Wyświetlanie informacji on-line o statusie monitorowanych końcówek | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | • System powinien obsługiwać agenta w formie<br>o Stałej (Presistent Agent)<br>o Tymczasowej (Dissolvabe Agent)<br>o Agenta NAP<br>W ramach wdrożenia Zamawiający wymaga:<br>1. Zapoznania się konfiguracją dotychczasowego sprzętu zainstalowanego w siedzibie Zamawiającego w celu opracowania strategii konfiguracji docelowego urządzenia wraz z przeniesieniem konfiguracji oraz polityk z dotychczasowego urządzenia UTM Zamawiającego do nowego urządzenia;<br>2. Dostosowania wszystkich polityk do opcji dostępnych w najnowszym firmware, po uprzednim omówieniu nowych i brakujących opcji w dotychczasowej konfiguracji Zamawiającego;<br>3. Wykonania testów poprawności konfiguracji oraz usunięcie zaistniałych błędów konfiguracji i problemów w funkcjonowaniu urządzenia oraz dostępu do sieci;<br>4. Dostosowania konfiguracji oraz polityk do środowiska Zamawiającego do pełnej integracji z systemem zarządzania nowego UTM.<br>5. W ramach wdrożenia Zamawiający wymaga zintegrowania wdrażanego rozwiązania zarządzającego infrastrukturą sieciową z posiadanym przez zamawiającego urządzeniem firewall firmy Fortinet. Integracja ma umożliwiać automatyczną kontrolę urządzeń sieciowych w oparciu o zdarzenia wykryte przez firewall. Automatyczne działania mają dotyczyć zdarzeń związanych z kontrolą antywirusową, IPS oraz DoS.<br>6. Wymagane funkcjonalności:<br>• Całkowite blokowanie wskazanych hostów na poziomie gniazdka switcha; przenoszenie wskazanych hostów do odseparowanych VLAN;<br>• Wprowadzanie informacji na temat wprowadzonych zmian do bazy będącej częścią systemu zarządzania;<br>• Informowanie o przeprowadzonych operacjach poprzez email;<br>• W przypadku separacji hosta, wymagana jest możliwość powiadomienia użytkownika hosta poprzez przekierowanie http | |
| 17. | Opisy do wymagań ogólnych | 1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (t.j. Dz.U.2022.1666 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | 2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

**8.** Przełącznik sieciowy – 5 szt.

| Lp. | Nazwa komponentu | Wymagane parametry techniczne | Oferowane parametry techniczne |
|---|---|---|---|
| | | **Dane ogólne** | |
| 1. | Dane ogólne | Sprzęt niezbędny do zastosowań poprawy bezpieczeństwa dystrybucji w sieci LAN Zamawiającego | Producent ……<br><br>Nazwa i model ……<br><br>Zamawiający wymaga dołączenia do oferty dokumentów:<br>Karta produktu |
| 2. | Porty | • 24 porty RJ45 10/100/1000 Mb/s<br>• 4 sloty SFP+ 10 Gb/s<br>• 1 port konsolowy RJ45<br>• 1 port konsolowy microUSB | Spełnia Tak*/Nie* |
| 3. | Bezwentylatorowy | Tak | Spełnia Tak*/Nie* |
| 4. | Zasilanie | 100-240 V AC~50/60 Hz | Spełnia Tak*/Nie* |
| 5. | Wymiary (S x G x W) | 440 × 180 × 44 mm (17,3 × 7,1 × 1,7 cala) | Spełnia Tak*/Nie* |
| 6. | Montaż | Możliwość montażu w szafie rack | Spełnia Tak*/Nie* |
| 7. | Maks. zużycie energii | 23,6 W (110V/60 Hz) | Spełnia Tak*/Nie* |
| 8. | Ilość generowanego ciepła | 80,353 BTU/h (110 V/60 Hz) | Spełnia Tak*/Nie* |
| 9. | Wydajność | | |
| 10. | Wydajność przełączania | 128 Gb/s | Spełnia Tak*/Nie* |
| 11. | Szybkość przekierowań pakietów | 95,23 Mp/s | Spełnia Tak*/Nie* |
| 12. | Tablica adresów MAC | 16 K | Spełnia Tak*/Nie* |
| 13. | Bufor pakietów | 12 Mbit | Spełnia Tak*/Nie* |
| 14. | Ramki jumbo | 9 KB | Spełnia Tak*/Nie* |
| 15. | Funkcja Quality of Service | • 8 kolejek priorytetowania<br>• Obsługa priorytetowania 802.1p CoS/DSCP<br>• Tryb harmonogramu priorytetowania:<br>- SP (Strict Priority)<br>- WRR (Weighted Round Robin)<br>- SP+WRR<br>• Kontrola przepustowości | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | - Ograniczanie prędkości transferu w oparciu o port/przepływ danych<br>• Płynniejsze działanie<br>• Działania dla przepływów<br>- Mirror (do obsługiwanego interfejsu)<br>- Redirect (do obsługiwanego interfejsu)<br>- Limit prędkości<br>- Boss Remark | |
| 16. | L2 Multicast | • IGMP Snooping<br>- IGMP v1/v2/v3 Snooping<br>- Fast Leave<br>- IGMP Snooping Querier<br>- Uwierzytelnianie IGMP<br>• Uwierzytelnianie IGMP<br>• MVR<br>• MLD Snooping<br>- MLD v1/v2 Snooping<br>- Fast Leave<br>- MLD Snooping Querier<br>- Konfiguracja grupy statycznej<br>- Ograniczone przekazywanie IP Multicast<br>• Filtrowanie transmisji Multicast: 256 profili i 16 wpisów na profil | Spełnia Tak*/Nie* |
| 17. | Sieci VLAN | • Grupy VLAN<br>- Maks. 4K grup VLAN<br>• Tagowanie 802.1Q VLAN<br>• Adres MAC VLAN: 7 wpisów<br>• Protokół VLAN<br>• Prywatna sieć VLAN<br>• GVRP<br>• VLAN VPN (QinQ)<br>- QinQ oparty na portach<br>- Selective QinQ<br>• Głosowa sieć VLAN | Spełnia Tak*/Nie* |
| 18. | Listy kontroli dostępu | • Lista kontroli dostępu (ACL) oparta o czas<br>• Adres MAC ACL<br>- Źródłowy adres MAC<br>- Docelowy adres MAC<br>- ID sieci VLAN | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | - User Priority<br>- Ethertype<br>• Adres IP ACL<br>- Źródłowy adres IP<br>- Docelowy adres IP<br>- Fragment<br>- Protokół IP<br>- Flaga TCP<br>- Port TCP/UDP<br>- TOS DSCP/IP<br>- User Priority<br>• ACL IPv6<br>• ACL zawartości pakietu<br>• Łączona ACL<br>• Polityka kontroli dostępu<br>- Mirroring<br>- Limit prędkości<br>- Redirect<br>- QoS Remark<br>• ACL do portu/VLAN | |
| 19. | Bezpieczeństwo transmisji | • Wiązanie adresów IP, MAC i portów<br>- 512 wpisów<br>- DHCP Snooping<br>- Inspekcja ARP<br>- Ochrona źródłowego adresu IPv4: 100 wpisów<br>• Wiązanie adresów IPv6, MAC i portów<br>- 512 wpisów<br>- DHCPv6 Snooping<br>- Wykrywanie ND<br>- Ochrona źródłowego adresu IPv6: 100 wpisów<br>• Ochrona przed atakami DoS<br>• Ochrona portów poprzez ich statyczną/dynamiczną/stałą konfigurację<br>- Do 64 adresów MAC na port<br>• Storm Control Broadcast/Multicast/Unicast<br>- tryb kontroli (kb/s/wskaźnik)<br>• Uwierzytelnianie 802.1X<br>- Uwierzytelnianie w oparciu o port | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | - Uwierzytelnianie w oparciu o adres MAC<br>- Przydzielanie VLAN<br>- MAB<br>- Sieć VLAN dla gości<br>- Uwierzytelnianie i autoryzowanie poprzez Radius<br>• AAA (w tym TACACS+)<br>• Izolacja portów<br>• Bezpieczne zarządzanie webowe poprzez HTTPS z szyfrowaniem SSLv3/TLS 1.2<br>• Bezpieczne zarządzanie CLI z szyfrowaniem SSHv1/SSHv2<br>• Kontrola dostępu w oparciu o IP/port/MAC | |
| 20. | IPv6 | • IPv6 Dual IPv4/IPv6<br>• Multicast Listener Discovery (MLD) Snooping<br>• ACL IPv6<br>• Interfejs IPv6<br>• Statyczny routing IPv6<br>• Funkcja neighbor discovery (ND) wykorzystywana przez węzły IPv6<br>• Path maximum transmission unit (MTU) discovery<br>• ICMP v6<br>• TCP v6/UDP v6<br>• Zastosowania protokołu IPv6:<br>- Klient DHCPv6<br>- Ping6<br>- Tracert6<br>- Telnet (v6)<br>- SNMP IPv6<br>- SSH IPv6<br>- SSL IPv6<br>- Http/Https<br>- TFTP IPv6 | Spełnia Tak*/Nie* |
| 21. | Cechy przełącznika L3 | • 16 interfejsów IPv4/IPv6<br>• Routing statyczny<br>- 48 tras statycznych<br>• Wpisy statyczne ARP<br>- 128 wpisów statycznych<br>• Proxy ARP<br>• Gratuitous ARP<br>• Serwer DHCP | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | • DHCP Relay<br>- DHCP Interface Relay<br>- DHCP VLAN Relay<br>• DHCP L2 Relay | |
| 22. | Zarządzanie | • Interfejs graficzny GUI<br>• Interfejs linii poleceń CLI przez port konsolowy i telnet<br>• SNMP v1/v2c/v3<br>- Trap/Inform<br>- RMON (grupy 1,2,3,9)<br>• Szablon SDM<br>• Klient DHCP/BOOTP<br>• LLDP/LLDP-MED 802.1ab<br>• Automatyczna instalacja DHCP<br>• Dual Image, Dual Configuration<br>• Monitorowanie zużycia procesora<br>• Diagnostyka kabli<br>• EEE<br>• Odzyskiwanie haseł<br>• SNTP<br>• Logi systemu | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

## 9. Serwer wraz z oprogramowaniem – 2 szt.

| Lp. | Parametr | Charakterystyka (wymagania minimalne) | Parametr oferowany |
|---|---|---|---|
| 1. | Obudowa | Obudowa Tower z możliwością instalacji do minimum 3 dysków 3.5" Hot-Plug. Posiadająca dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera. | Producent: ……<br>Model i wersja: ……<br><br>Zamawiający wymaga dołączenia do oferty dokumentów:<br>Karta produktu |
| 2. | Płyta główna | Płyta główna z możliwością zainstalowania minimum jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. | Spełnia Tak*/Nie* |
| 3. | Chipset | Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych. | Spełnia Tak*/Nie* |
| 4. | Procesor | Zainstalowany jeden procesor czterordzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 10.5 punktów w teście SPECspeed®2017_int_base dostępnym na stronie www.spec.org. Do oferty należy załączyć wydruk ze strony potwierdzający osiągnięty wynik dla oferowanego modelu serwera | Spełnia Tak*/Nie* |
| 5. | RAM | Minimum 32GB na płycie głównej powinno znajdować się minimum 2 wolne sloty przeznaczone do rozbudowy pamięci. Płyta główna powinna obsługiwać do 64GB pamięci RAM. | Spełnia Tak*/Nie* |
| 6. | Zabezpieczenia pamięci RAM | Memory Rank Sparing, Memory Mirror, Lockstep | Spełnia Tak*/Nie* |
| 7. | Gniazda PCI | Min. PCI-e x16 - 1 szt. PCI-e x4 - 2 szt. PCI - 1 szt | Spełnia Tak*/Nie* |
| 8. | Interfejsy sieciowe | Wbudowany minimum 1 porty typu Gigabit Ethernet Base-T. | Spełnia Tak*/Nie* |
| 9. | Napęd optyczny | Wbudowany DVD-RW | Spełnia Tak*/Nie |
| 10. | Dyski twarde | Możliwość instalacji dysków SATA, SSD. Zainstalowany minimum 1 dysk 512GB PCIe z radiatorem | Spełnia Tak*/Nie |
| 11. | Kontroler RAID | Wirtualny kontroler dyskowy, możliwe konfiguracje poziomów RAID: min 0, 1, 5, 10 | Spełnia Tak*/Nie |
| 12. | Wbudowane porty | Przedni panel : minimum 2 USB 2.0 Type-A , 1 USB 3.0 Type-A 1x USB 3.1 Type-C<br>Tylny panel obudowy : 4 porty zgodne z USB 3.0 typu A 2 porty zgodne ze standardem USB 2.0 typu<br>Minimum 1 port DisplayPort znajdujący się na tylnym panelu | Spełnia Tak*/Nie |
| 13. | Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 | Spełnia Tak*/Nie |
| 14. | Wentylatory | Minimum 1 wentylator | Spełnia Tak*/Nie |
| 15. | Zasilacz | Zasilacz maksymalnie 300 W | Spełnia Tak*/Nie |
| 16. | Diagnostyka | Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji min. O pracy napędów, awarii podzespołów | Spełnia Tak*/Nie |
| 17. | System Operacyjny | Zamawiający wymaga dostarczenia Oprogramowania: Microsoft Windows Serwer Essential 2019, o następujących parametrach lub równoważnego, spełniającego kryteria oceny równoważności | Spełnia Tak*/Nie |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | Metryka licencyjna: per server<br>Rodzaj licencji: bezterminowa<br>Przez oprogramowanie równoważne Zamawiający rozumie oprogramowanie spełniające następujące warunki poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:<br>- Obsługa do 64GB RAM,<br>- Obsługa 2 CPU (bez ograniczenia liczby rdzeni),<br>- Możliwość obsługi maksymalnie 25 użytkowników i 50 urządzeń,<br>- Oprogramowanie nie może wymagać dodatkowych licencji w celu uzyskania dostępu do serwera Współpraca z procesorami o architekturze x86-64,<br>- Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym,<br>- Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory,<br>- Zawarta możliwość uruchomienia roli serwera DNS,<br>- Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP),<br>- Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory,<br>Zawarta możliwość uruchomienia roli serwera stron WWW. | |
| 18. | Certyfikaty | Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001.<br>Serwer musi posiadać deklaracja CE.<br>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Windows Server 2016 x64, Windows Server 2019 x64. | Spełnia Tak*/Nie* |
| 19. | Warunki gwarancji | Minimum 12 m-cy realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta.<br>Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.<br>. | **Pozycja podlegająca kryterium oceny ofert**<br><br>Spełnia Tak*/Nie*<br><br>Zamawiający wymaga dołączenia do oferty dokumentów:<br>Certyfikat ISO 9001 na świadczenie usług serwisowych<br>Dokument potwierdzający, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta |
| 20. | Wsparcie techniczne i oprogramowanie | Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego, automatycznie tworzące zgłoszenia serwisowe w przypadku awarii. | Producent …….. |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera.<br>Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów.<br><br>Konfiguracja i zaoferowany poziom wsparcia powinien po wystąpieniu awarii urządzenia automatycznie zakładać zlecenie serwisowe w dziale wsparcia producenta, poinformować o tym za pomocą wiadomości e-mail, a następnie dział wsparcia powinien się kontaktować z klientem w celu rozwiązania problemu.<br>Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające :<br>• Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień.<br>• Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów.<br>• Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta.<br>• upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,<br>• możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji :<br>a. o poprawkach i usprawnieniach dotyczących aktualizacji<br>b. dacie wydania ostatniej aktualizacji<br>c. priorytecie aktualizacji<br>d. zgodność z systemami operacyjnymi<br>e. jakiego komponentu sprzętu dotyczy aktualizacja<br>f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.<br>• wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne<br>• możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.<br>• rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty ( dd-mm-rrrr )<br>• sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą ( dd-mm-rrrr ) i wersją ( rewizja wydania )<br>• dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml<br>raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od | Nazwa i wersja oprogramowania<br>…….<br><br>Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą ( dd-mm-rrrr ) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku. | |
| 21. | Płyta główna | Płyta główna musi być zaprojektowana przez Producenta serwera i oznaczona jego logiem firmowym. | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

## 10. Szkolenie on-line dla pracowników działu IT w zakresie obsługi dostarczonego sprzętu i oprogramowania

| Lp. | Parametr | Wymagania minimalne | Oferowane parametry |
|---|---|---|---|
| 1. | Sposób organizacji szkolenia | Szkolenie zamknięte. | Spełnia Tak*/Nie* |
| 2 | Sposób organizacji szkolenia | Szkolenie przeprowadzone w języku polskim. | Spełnia Tak*/Nie* |
| 3. | Sposób organizacji szkolenia | Szkolenia muszą odbyć się w formie zdalnej poprzez udostępniony przez Wykonawcę kanał elektroniczny lub dedykowaną aplikację, z możliwością późniejszego odtworzenia spotkania (nagranie szkolenia), z zastrzeżeniem nierozpowszechniania nagrania poza obszar organizacji Zamawiającego. | Spełnia Tak*/Nie* |
| 4. | Sposób organizacji szkolenia | Szkolenie musi tworzyć cykl 5 (słownie pięciu) etapów, gdzie łączna liczba godzin poświęcona na szkolenie nie może być mniejsza niż 25 godzin | Spełnia Tak*/Nie* |
| 5. | Sposób organizacji szkolenia | Wykonawca gwarantuje, że osoba prowadząca szkolenia posiada wyczerpującą wiedzę, co najmniej na poziomie wymaganym do realizacji szkoleń w zakresie obsługi dostarczonego sprzętu i oprogramowania. | Spełnia Tak*/Nie* |
| 6. | Sposób organizacji szkolenia | Wykonawca jest zobowiązany przeprowadzić szkolenie w oparciu o zaakceptowane przez Zamawiającego tematy. | Spełnia Tak*/Nie* |
| 7. | Sposób organizacji szkolenia | Wykonawca zobowiązany jest w porozumieniu z Zamawiającym ustalić dokładną datę przeprowadzenia szkoleń. Zamawiający ustali na zasadzie negocjacji z Wykonawcą, w terminie maksymalnie 15 dni roboczych od daty podpisania umowy ramowy harmonogram szkoleń. | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

## 11. Stacja robocza typu laptop dedykowana do administrowania oprogramowaniem do zarządzania infrastrukturą IT – 1 szt.

| Szczegółowy opis | | | Parametry oferowane |
|---|---|---|---|
| Komputer przenośny.<br>W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy (numer konfiguracji lub part numer) oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. Jeśli na stronie internetowej producenta nie jest dostępna pełna oferta modeli sprzętu wraz z jego konfiguracją, do oferty należy dołączyć katalog producenta zaoferowanego produktu umożliwiający weryfikację oferty pod kątem zgodności z wymaganiami Zamawiającego. | | | Producent:<br>……<br>Model i wersja:<br>……<br>Numer katalogowy (numer konfiguracji lub part numer):<br>……<br>Zamawiający wymaga dołączenia do oferty dokumentów:<br>Karta produktu |
| Nie dopuszcza się modyfikacji na drodze Producent-Zamawiający. | | | Spełnia Tak*/Nie* |
| Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami SWZ. W tym celu Wykonawcy na wezwanie Zamawiającego dostarczą do siedziby Zamawiającego w terminie 5 dni od daty otrzymania wezwania, próbkę oferowanego sprzętu. W odniesieniu do programowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Ocena złożonych próbek zostanie dokonana na zasadzie spełnia / nie spełnia. Z badania każdej próbki zostanie sporządzony protokół. Pozytywna ocena próbki będzie oznaczała zgodność próbki (oferty) z treścią SWZ. Niezgodność próbki z SWZ, chociażby w zakresie jednego parametru podlegającemu badaniu bądź nieprzedłożenie wymaganej próbki w sposób i terminie wymaganym przez Zamawiającego będzie oznaczało negatywny wynik oceny próbki i będzie skutkowało odrzuceniem oferty na podstawie art. 226 ust. 1 pkt 5 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz.U.2022. 1710 ze zm.), tj. z uwagi na fakt, że treść oferty jest niezgodna z warunkami zamówienia. Szczegółowy sposób przygotowania i złożenia próbek zostanie dostarczony Wykonawcom wraz z wezwaniem do złożenia próbek | | | Spełnia Tak*/Nie* |
| Zamawiający zastrzega sobie prawo do sprawdzenia reżimu gwarancyjnego oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu. | | | Linki do stron producenta umożliwiające weryfikację reżimu gwarancyjnego oraz dostarczonej konfiguracji:<br>…… |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** | **Parametry** |
| 1 | Procesor | Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w mobilnych stacjach roboczych klasy x86, o wydajności liczonej w punktach równej lub wyższej procesorowi Intel Core i7-1260P na podstawie PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. | Spełnia Tak*/Nie* |
| 2 | Pamięć operacyjna RAM | Min. 32GB 3200MHz non-ECC, Pamięć RAM działająca w trybie dual-channel. | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| 3 | Parametry pamięci masowej | M.2 1TB SSD PCIe 3.0 NVMe OPAL2.0 | Spełnia Tak*/Nie* |
| 4 | Karta graficzna | Zintegrowana Intel Iris Xe Graphics lub równoważna | Spełnia Tak*/Nie* |
| 5 | Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki Dolby Audio, Port słuchawek i mikrofonu typu COMBO, kamera video HD | Spełnia Tak*/Nie* |
| 6 | Obudowa | Wykonana z materiałów o podwyższonej odporności na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych, charakteryzujący się wzmocnioną konstrukcją | Spełnia Tak*/Nie* |
| 7 | Płyta główna | Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej. | Spełnia Tak*/Nie* |
| 8 | Zgodność z systemami operacyjnymi | Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera ). | Spełnia Tak*/Nie* |
| 9 | Bezpieczeństwo | Zintegrowany z płytą główną 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 zapisanego w TPM2.0 z certyfikacją TCG. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej.<br>Dostęp do podzespołów komputera musi być sygnalizowany przez czujnik otwarcia obudowy. Sygnalizacja konfigurowana z poziomu BIOS. Zamawiający uzna za równoważne dostarczenie linki zabezpieczającej typu Kensington zamykanej w taki sposób, że nie będzie możliwe otwarcie obudowy notebooka, gdy linka zabezpieczająca zostanie umieszczona i zamknięta z wykorzystaniem kluczyka w dedykowanym slocie Kensington. Komputery wyposażone w złącze Noble Lock muszą zostać zaoferowane z adapterem ze złącza Noble Lock komputera do Kensington. | Spełnia Tak*/Nie* |
| 11 | Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji). | Spełnia Tak*/Nie* |
| 12 | BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera.<br>Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:<br>- wersji BIOS,<br>- daty produkcji BIOS,<br>- nr seryjnym komputera,<br>- ilości zainstalowanej pamięci RAM oraz możliwość odczytania informacji o obłożeniu, szybkości i rodzaju z poziomu BIOS lub w zaimplementowanym systemie diagnostycznym,<br>- typie procesora i jego prędkości,<br>- MAC adresu zintegrowanej karty sieciowej,<br>- nr inwentarzowym (tzw. Asset Tag) - wymagane wolne pole do edycji przez administratora, | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | - nr seryjnym płyty głównej komputera,<br>- informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS. | |
| 13 | Ekran | Matowy, matryca TFT 14" z podświetleniem w technologii LED, rozdzielczość 1920x1200, 400nits, kontrast 1000:1 w technologii IPS lub PLS lub WVA, Kąt otwarcia pokrywy ekranu min.180 stopni. | Spełnia Tak*/Nie* |
| 14 | Interfejsy / Komunikacja | 2xUSB 3.2 Gen.1, 2x USB-C z Thunderbolt 4, złącze słuchawek i złącze mikrofonu typu COMBO, HDMI min. 2.0, RJ-45, czytnik smart card reader (kart inteligentnych) Złącze umożliwiające podpięcie linki antykradzieżowej. | Spełnia Tak*/Nie* |
| 15 | Karta sieciowa LAN | 10/100/1000 wspierająca Wake on Lan, PXE Boot, HTTPs | Spełnia Tak*/Nie* |
| 16 | Karta sieciowa WLAN | Wbudowana karta sieciowa, pracująca w standardzie Wifi 6E<br>Bluetooth 5.2 | Spełnia Tak*/Nie* |
| 18 | Klawiatura i touchpad | Podświetlana klawiatura w układzie US, wielodotykowy touchpad | Spełnia Tak*/Nie* |
| 19 | Czytnik linii papilarnych | Wbudowany czytnik linii papilarnych – wspierający dwupoziomową preautentykację w BIOS. | Spełnia Tak*/Nie* |
| 20 | Akumulator | Komputer ma być wyposażony w system szybkiego ładowania akumulatora, który umożliwia szybkie naładowanie akumulatora notebooka do 80% w ciągu 60 minut. Akumulator o pojemności min. 52Wh. | Spełnia Tak*/Nie* |
| 21 | Zasilacz | Zasilacz zewnętrzny min 90W | Spełnia Tak*/Nie* |
| 22 | Certyfikaty, oświadczenia i standardy | Dla producenta sprzętu należy dostarczyć certyfikat:<br>ISO 9001<br>ISO 14001<br>Deklaracja zgodności CE (załączyć do oferty)<br>Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki<br>Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy Operating CPU wynosząca maksymalnie 18 dB (załączyć oświadczenie producenta lub raport głośności) | Spełnia Tak*/Nie* |
| 23 | Waga/Wymiary | Waga urządzenia z akumulatorem max. 1.36 kg wg karty katalogowej producenta.<br>Grubość notebooka nie większa niż: 21 mm. | Spełnia Tak*/Nie* |
| 24 | System operacyjny | System operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:<br>1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:<br>a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,<br>b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych<br>2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego<br>3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim | Spełnia Tak*/Nie*<br><br>Producent:<br>……<br>Nazwa i wersja oprogramowania:<br>…… |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.<br>5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe<br>6. 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,<br>7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.<br>8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim<br>9. Wbudowany system pomocy w języku polskim.<br>10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).<br>11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.<br>12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.<br>13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.<br>14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.<br>15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze, z pełną obsługą Zasad grupowych<br>16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".<br>17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.<br>18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.<br>19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.<br>20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.<br>21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.<br>22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.<br>23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).<br>24. Wbudowany mechanizm wirtualizacji typu hypervisor.<br>25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.<br>26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. | |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.<br>28. 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.).<br>29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.<br>30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.<br>31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.<br>32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM<br>33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.<br>34. Możliwość tworzenia wirtualnych kart inteligentnych.<br>35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)<br>36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.<br>37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.<br>38. Mechanizmy logowania w oparciu o:<br>a. Login i hasło,<br>b. Karty inteligentne i certyfikaty (smartcard),<br>c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),<br>d. Certyfikat/Klucz i PIN<br>e. Certyfikat/Klucz i uwierzytelnienie biometryczne<br>39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5<br>40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.<br>41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach<br>42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń<br>43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń | |
| 25 | Oprogramowanie do aktualizacji sterowników | Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. | Spełnia Tak*/Nie* |
| 26 | Gwarancja | Minimalny czas trwania wsparcia technicznego producenta wynosi 3 lata – podjęcie próby naprawy na następny dzień roboczy. | Spełnia Tak*/Nie* |



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

| | | | |
|---|---|---|---|
| | | Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.<br>Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. | Zamawiający wymaga dołączenia do oferty dokumentów:<br>Certyfikat ISO 9001 na świadczenie usług serwisowych<br>Dokument potwierdzony przez Producenta, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta |
| 27 | Wsparcie techniczne producenta | Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera<br>Bezpośredni kontakt z Autoryzowanym Partnerem Serwisowym Producenta (brak konieczności zgłaszania każdej usterki sprzętowej telefonicznie), mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki.<br>Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00-18:00<br>Wsparcie techniczne świadczone przez producenta lub autoryzowanego partnera serwisowego dla urządzeń i preinstalowanego oprogramowania OEM, zakupionego z urządzeniem, dostarczane zdalnie.<br><br>Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta.<br>Przydzielenie zasobu w postaci kierownika technicznego w przypadku eskalacji problemów serwisowych.<br><br>Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta. | Spełnia Tak*/Nie* |

Mariola Szczęsna; Gmina i Miasto Lwówek Śląski

Elektronicznie podpisany przez Mariola Szczęsna; Gmina i Miasto Lwówek Śląski
Data: 2023.08.07 13:19:14 +02'00'



Fundusze Europejskie Polska Cyfrowa
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19