**Załącznik 1a do zapytania ofertowego 1/12/2024/CUS**

**Specyfikacja techniczna zamówienia (STZ)**

**Część 1: Sprzęt komputerowy, informatyczny i oprogramowanie**

**Spis treści**

[1. Laptop TYP I – 1 szt. 2](#_Toc185453747)

[2. Laptop TYP II – 2 szt. z oprogramowaniem zabezpieczającym (programem antywirusowym – 2 licencje) 7](#_Toc185453748)

[3. Oprogramowanie biurowe – 2 licencje 13](#_Toc185453749)

[4. UPS do laptopów – 2 szt. 13](#_Toc185453750)

Do:

Gmina Mrocza

działająca poprzez realizatora:

Miejsko-Gminny Ośrodek Pomocy Społecznej w Mroczy

przekształcony w Centrum Usług Społecznych w Mroczy

ul. Łąkowa 7, 89-115 Mrocza

**WYKONAWCA:**

|  |  |
| --- | --- |
| Pełna nazwa albo  imię i nazwisko Wykonawcy  (wpisz dane zgodne z dokumentami rejestrowymi): |  |
| Siedziba albo miejsce zamieszkania i adres Wykonawcy  (wpisz dane zgodne z dokumentami rejestrowymi) |  |
| Nr telefonu/faksu: |  |
| Adres e-mail: |  |
| NIP/REGON/PESEL (jeśli dotyczy): |  |
| Osoba upoważniona do kontaktów (imię, nazwisko, tel. adres e-mail): |  |

# Laptop TYP I – 1 szt.

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry (potwierdź spełnienie poprzez skreślenie niepoprawnej odpowiedzi) oraz wpis wymagane dane według wskazań** |
|  | Ekran | Min. 15.6” LED IPS FHD o rozdzielczości 1920x1080, z powłoką matową, nie dopuszcza się matryc typu "glare". Matryca komputera otwierana do 180 stopni. | **Producent**  **Nazwa /model** |
|  | Wydajność komputera | Oferowany komputer przenośny musi osiągać w teście wydajności :  SYSMARK 25 – wynik min. 1200 – **test oferowanej konfiguracji wymagany do załączenia na etapie umowy z Wykonawcą.**  Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS ( tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).  Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego | **Podać wartość w punktach**  SPEŁNIA  TAK /NIE |
|  | Chipset | Zaprojektowany i wykonany do pracy w komputerach przenośnych rekomendowany przez producenta procesora. | SPEŁNIA  TAK /NIE |
|  | Obudowa | Dopuszczalne kolory – czarny/srebrny. | SPEŁNIA  TAK /NIE |
|  | Pamięć RAM | 32GB DDR4 (nie dopuszcza się wlutowanych pamięci w płytę główną). | SPEŁNIA  TAK /NIE |
|  | Dysk twardy | Min. 512GB SSD  Dysk twardy musi zawierać partycję recovery – na partycji musi znajdować się obraz zainstalowanych i skonfigurowanych elementów tj.:  - systemu operacyjnego  - oprogramowania antywirusowego  Partycja musi zapewniać przywrócenie systemu operacyjnego, zainstalowanego i skonfigurowanego w/w oprogramowania.  Możliwość instalacji wewnątrz obudowy drugiego dysku 2.5. | SPEŁNIA  TAK /NIE |
|  | Karta graficzna | Karta graficzna powinna umożliwiać pracę dwumonitorową ze wsparciem DirectX 12, OpenGL 4.5, osiągająca w teście PC Mark 10 Digital Content Creation wynik min. 5000 pkt - **test oferowanej konfiguracji wymagany do załączenia na etapie umowy z Wykonawcą.** | **Podać wartość w punktach**  SPEŁNIA  TAK /NIE |
|  | Karta dźwiękowa | Karta dźwiękowa zgodna z HD Audio, wbudowane dwa głośniki stereo oraz dwa cyfrowe mikrofony | SPEŁNIA  TAK /NIE |
|  | Wbudowane połączenia i karty sieciowe | Karta sieciowa LAN 10/100/1000 LAN  WLAN 6E 802.11ax wraz z Bluetooth 5.2 | SPEŁNIA  TAK /NIE |
|  | Porty/złącza  (wbudowane) | 1x Złącze RJ-45 (podłączenie sieci lokalnej)  1x Czytnik Kart pamięci SD  1x USB-C 3.2 (z DisplayPort oraz z możliwością ładowania Baterii laptopa)  3x USB 3.2  1x Gniazdo mikrofonowe/Gniazdo słuchawkowe (Combo)  1x HDMI ze wsparciem HDCP  1x zasilanie DC-in | SPEŁNIA  TAK /NIE |
|  | Klawiatura | Pełnowymiarowa klawiatura podświetlana z wydzielonymi pełnowymiarowymi klawiszami numerycznymi w prawej części klawiatury, w układzie US-QWERTY, polskie znaki zgodne z układem MS Windows "polski programistyczny", klawiatura podświetlana musi być wyposażona w 2 klawisze ALT (prawy i lewy). | SPEŁNIA  TAK /NIE |
|  | Urządzenie wskazujące | Touch Pad (płytka dotykowa) wbudowana w obudowę notebooka.  Czytnik linii papilarnych | SPEŁNIA  TAK /NIE |
|  | Kamera | Wbudowana, o parametrach:  HD 1280x720, 720p HD audio/video nagrywanie. Wbudowane dwa kierunkowe mikrofony, mechaniczna przesłona kamery. | SPEŁNIA  TAK /NIE |
|  | Bateria | Litowo-jonowa – czas pracy min. 12h wyników testów BAPCO MobileMark 25 – **test należy dołączyć na etapie umowy z Wykonawcą** | SPEŁNIA  TAK /NIE |
|  | Zasilacz | Zewnętrzny, pracujący w sieci elektrycznej 230V 50/60Hz, max 90W. | SPEŁNIA  TAK /NIE |
|  | Obudowa waga i wymiary | Waga nie większa niż 1,8kg, grubość nie przekraczająca 20mm. Obudowa wzmocniona, szkielet wykonany ze wzmocnionego aluminium.  Obudowa musi spełniać standard MIL-STD 810G (potwierdzony w oficjalnych dokumentach producenta **lub wynikiem z przeprowadzonych testów - wymagane do załączenia na etapie umowy z Wykonawcą**) | SPEŁNIA  TAK /NIE |
|  | Bezpieczeństwo | - Zabezpieczenie BIOS hasłem użytkownika.  - Zabezpieczenie dysku twardego hasłem użytkownika.  - Złącze typu Kensington Lock.  - Zintegrowany z płytą główną dedykowany 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 - Trusted Platform Module 2.0. | SPEŁNIA  TAK /NIE |
|  | System operacyjny | Zainstalowany system operacyjny Windows 11 Professional lub równoważny  Parycja Recovery umożliwiająca w przypadku awarii dysku twardego ponowną instalację zainstalowanego systemu operacyjnego oraz nośnik zawierający sterowniki wszystkich zainstalowanych urządzeń  Windows 11 Professional lub równoważny:  System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego  3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim  4. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe  5. 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,  6. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.  7. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim  8. Wbudowany system pomocy w języku polskim.  9. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).  10. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące  11. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń  12. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń  13. Możliwość pracy w domenie Active Directory | **Producent**  **Nazwa i wersja oprogramowania**  SPEŁNIA  TAK /NIE |
|  | Certyfikaty i standardy | * Certyfikat ISO 9001, 14001, 50001 dla producenta sprzętu **(wymagany do załączenia na etapie umowy z Wykonawcą).** * Deklaracja zgodności CE i ROHS **(wymagany do załączenia na etapie umowy z Wykonawcą).** * Standard MIL-STD-810G (potwierdzony w oficjalnych dokumentach producenta **lub wynikiem z przeprowadzonych testów - wymagane do załączenia na etapie umowy z Wykonawcą)** | SPEŁNIA  TAK /NIE |
|  | Dodatkowe oprogramowanie zabezpieczające | System chroniący przed zagrożeniami, posiadający certyfikaty: OPSWAT Platinum, AV-Test ‘Top Product’, AV Comperative Advance +, ISO 27001 .  Szyfrowanie danych:  •Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.  •Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.  Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.  Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.  Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.  Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.  Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.  Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.  Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.  Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware  Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:  • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli  • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory  • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux  • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.  • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich  • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji  Zarządzanie przez Chmurę:  1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach  2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury  3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur  4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy  5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach  6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń  7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej  Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.  Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.  1.Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer  2.Oprogramowanie klienckie, zarządzane z poziomu serwera.  System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:  • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie  • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD  • funkcje regulowania połączeń WiFi i Bluetooth  • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe  • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi  • funkcje blokowania dostępu dowolnemu urządzeniu  • możliwość tymczasowego dodania dostępu do urządzenia przez administratora  • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu  • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka  • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora  • możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry  • możliwość używania tylko zaufanych urządzeń sieciowych,w tym urządzeń wskazanych na końcówkach klienckich  • funkcję wirtualnej klawiatury  • możliwość blokowania każdej aplikacji  • możliwość zablokowania aplikacji w oparciu o kategorie  • możliwość dodania własnych aplikacji do listy zablokowanych  • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze  • dodawanie innych aplikacji  • dodawanie aplikacji w formie portable  • możliwość wyboru pojedynczej aplikacji w konkretnej wersji  • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB  • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool  • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.  • możliwość zablokowania funkcji Printscreen  • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx  • funkcje monitorowania i kontroli przepływu poufnych informacji  • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików  • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj  • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe  • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe  • ochrona zawartości schowka systemu  • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL  • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych  • ochrona plików zamkniętych w archiwach  • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem  • możliwość tworzenia profilu DLP dla każdej polityki  • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania  • ochrona przez wyciekiem plików poprzez programy typu p2p  Monitorowanie zmian w plikach:  • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.  • Funkcje monitorowania określonych rodzajów plików.  • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.  • Generator raportów do funkcjonalności monitora zmian w plikach.  • możliwość śledzenia zmian we wszystkich plikach  • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach  • możliwość definiowana własnych typów plików  Optymalizacja systemu operacyjnego stacji klienckich:  • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku  • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem  • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich  • instruktaż stanowiskowy pracowników Zamawiającego  • dokumentacja techniczna w języku polskim  Wspierane platformy i systemy operacyjne:  1.Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)  2.Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)  3.Mac OS X, Mac OS 10  4.Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat  Platforma do zarządzania dla Android i iOS:  • Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę  • Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.  Zarządzanie użytkownikiem  • Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email  • Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika  • Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi  • Musi posiadać możliwość eksportu danych użytkownika  Zarządzanie urządzeniem  • Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO  • Musi umożliwiać import listy urządzeń z pliku CSV  • Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych  • Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta  • Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał  • Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres  • Musi zawierać podgląd aktualnie zainstalowanych aplikacji  • Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych,  • Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł  • Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres  Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:  Wymagania dotyczące technologii:  1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową  2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.  3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:  - Microsoft Internet Explorer  - Microsoft Edge  - Mozilla Firefox  - Google Chrome  - Safari  4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących  5 Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie  6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:  - Windows 2008 R2  - Windows 2012  - Windows 2012 R2  - Windows 2016  7. Portal zarządzający musi umożliwiać:  a) przegląd wybranych danych na podstawie konfigurowalnych widgetów  b) zablokowania możliwości zmiany konfiguracji widgetów  c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.  d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności  e) eksport wszystkich skanów podatności do pliku CSV  Backup i przywracanie danych  - Deduplikacja danych,  - Backup przyrostowy i różnicowy,  - Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,  - Backup danych lokalnych – plikowy oraz poczty Outlook,  - Backup otwartych plików (VSS),  - Filtr plików oraz folderów,  - Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),  - Wyłączanie komputera po wykonaniu backupu,  - Przywracanie danych do wskazanej lokalizacji,  - Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,  - Wyszukiwanie plików w repozytorium użytkownika,  Ustawienia  - Automatyczne logowanie,  - Zapamiętywanie danych logowania,  - Automatyczne uruchamianie programu przy starcie systemu,  - Ustawianie priorytetu dla procesu backupu,  - Zmiana klucza szyfrującego,  - Ustawienia przepustowości/zajętości pasma,  - Konfiguracja wydajności procesu backupu,  Bezpieczeństwo  - Zastępowanie nazwy pliku GUID-em,  - Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,  - Kompresja danych,  - Transmisja po bezpiecznym protokole TLS,  - Deklaracja klucza szyfrującego dane użytkownika,  - Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,  - Obliczanie sumy kontrolnej,  - Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski.  WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze, Mac OS,Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji.  Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. | **Producent**  **Nazwa i wersja oprogramowania**  SPEŁNIA  TAK /NIE |
|  | Wsparcie techniczne producenta | 1. Dostęp do aktualizacji systemu BIOS, podręczników użytkownika, najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta komputera numeru seryjnego lub modelu komputera **– do oferty należy dołączyć link strony poprzez wpisanie go w kolumnie obok.** 2. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu Komputera. 3. W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy zestawu oraz podzespoły montowane przez Producenta były przez niego certyfikowane. Wykonawca niebędący producentem oferowanego sprzętu nie może samodzielnie dokonywać jego modyfikacji. | **Podaj link strony:**  **…………………………………..**  SPEŁNIA  TAK /NIE |
|  | Dodatkowe oprogramowanie | Wykonawca dostarczy wraz z komputerem oprogramowanie producenta komputera które umożliwia aktualizację sterowników, pełne zarządzanie, monitoring, konfigurację a w szczególności: dystrybucję ustawień BIOS (zawierającego wcześniej zdefiniowane ustawienia jednakowe dla wszystkich), jednocześnie na wszystkich komputerach zgodnie z polityką bezpieczeństwa Zamawiającego.  Wykonawca dostarczy sterowniki w formacie dedykowanym dla Microsoft SCCM w celu dystrybucji za pomocą dołączonego oprogramowania producenta komputera zgodnie z polityką bezpieczeństwa Zamawiającego.  Zamawiający oczekuje oprogramowania zarządzającego produkowanego przez producenta i instalowanego przez producenta na etapie produkcji komputera. Program ma umożliwiać przynajmniej:  - monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów  - powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu  - powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów  - śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem.  Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające:   * upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, * 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 o:   + poprawkach i usprawnieniach dotyczących aktualizacji   + dacie wydania ostatniej aktualizacji | **Producent**  **Nazwa i wersja oprogramowania**  SPEŁNIA  TAK /NIE |
|  | Gwarancja | Gwarancja producenta komputera min. 36 miesięcy  Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta – wymagane oświadczenie potwierdzające, że serwis będzie realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego producenta **(oświadczenie należy dołączyć na etapie umowy z Wykonawcą).**  Autoryzowany Partner Serwisowy musi posiadać status autoryzowanego partnera serwisowego producenta komputera.  Serwis urządzeń musi być realizowany zgodnie z wymogami normy ISO9001  Wymagane okno czasowe dla zgłaszania usterek min. wszystkie dni robocze w godzinach od 8:00 do 20:00. Zgłoszenie serwisowe przyjmowane poprzez stronę www lub telefoniczne (dedykowany numer serwisowy do obsługi zgłoszeń serwisowych. | SPEŁNIA  TAK /NIE |

# Laptop TYP II – 2 szt. z oprogramowaniem zabezpieczającym (programem antywirusowym – 2 licencje)

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry (potwierdź spełnienie poprzez skreślenie niepoprawnej odpowiedzi) oraz wpis wymagane dane według wskazań** |
|  | Ekran | Min. 15.6” LED IPS FHD o rozdzielczości 1920x1080, z powłoką matową, nie dopuszcza się matryc typu "glare". Matryca komputera otwierana do 180 stopni. | **Producent**  **Nazwa /model** |
|  | Wydajność komputera | Oferowany komputer przenośny musi osiągać w teście wydajności :  SYSMARK 25 – wynik min. 1200 – **test oferowanej konfiguracji wymagany do załączenia na etapie umowy z Wykonawcą.**  Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS ( tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).  Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego | **Podać wartość w punktach**  SPEŁNIA  TAK /NIE |
|  | Chipset | Zaprojektowany i wykonany do pracy w komputerach przenośnych rekomendowany przez producenta procesora. | SPEŁNIA  TAK /NIE |
|  | Obudowa | Dopuszczalne kolory – czarny/srebrny. | SPEŁNIA  TAK /NIE |
|  | Pamięć RAM | 16GB DDR4 (nie dopuszcza się wlutowanych pamięci w płytę główną). | SPEŁNIA  TAK /NIE |
|  | Dysk twardy | Min. 512GB SSD  Dysk twardy musi zawierać partycję recovery – na partycji musi znajdować się obraz zainstalowanych i skonfigurowanych elementów tj.:  - systemu operacyjnego  - oprogramowania antywirusowego  Partycja musi zapewniać przywrócenie systemu operacyjnego, zainstalowanego i skonfigurowanego w/w oprogramowania.  Możliwość instalacji wewnątrz obudowy drugiego dysku 2.5. | SPEŁNIA  TAK /NIE |
|  | Karta graficzna | Karta graficzna powinna umożliwiać pracę dwumonitorową ze wsparciem DirectX 12, OpenGL 4.5, osiągająca w teście PC Mark 10 Digital Content Creation wynik min. 5000 pkt - **test oferowanej konfiguracji wymagany do załączenia na etapie umowy z Wykonawcą.** | **Podać wartość w punktach**  SPEŁNIA  TAK /NIE |
|  | Karta dźwiękowa | Karta dźwiękowa zgodna z HD Audio, wbudowane dwa głośniki stereo oraz dwa cyfrowe mikrofony | SPEŁNIA  TAK /NIE |
|  | Wbudowane połączenia i karty sieciowe | Karta sieciowa LAN 10/100/1000 LAN  WLAN 6E 802.11ax wraz z Bluetooth 5.2 | SPEŁNIA  TAK /NIE |
|  | Porty/złącza  (wbudowane) | 1x Złącze RJ-45 (podłączenie sieci lokalnej)  1x Czytnik Kart pamięci SD  1x USB-C 3.2 (z DisplayPort oraz z możliwością ładowania Baterii laptopa)  3x USB 3.2  1x Gniazdo mikrofonowe/Gniazdo słuchawkowe (Combo)  1x HDMI ze wsparciem HDCP  1x zasilanie DC-in | SPEŁNIA  TAK /NIE |
|  | Klawiatura | Pełnowymiarowa klawiatura podświetlana z wydzielonymi pełnowymiarowymi klawiszami numerycznymi w prawej części klawiatury, w układzie US-QWERTY, polskie znaki zgodne z układem MS Windows "polski programistyczny", klawiatura podświetlana musi być wyposażona w 2 klawisze ALT (prawy i lewy). | SPEŁNIA  TAK /NIE |
|  | Urządzenie wskazujące | Touch Pad (płytka dotykowa) wbudowana w obudowę notebooka.  Czytnik linii papilarnych | SPEŁNIA  TAK /NIE |
|  | Kamera | Wbudowana, o parametrach:  HD 1280x720, 720p HD audio/video nagrywanie. Wbudowane dwa kierunkowe mikrofony, mechaniczna przesłona kamery. | SPEŁNIA  TAK /NIE |
|  | Bateria | Litowo-jonowa – czas pracy min. 12h wyników testów BAPCO MobileMark 25 – **test wymagany do załączenia na etapie umowy z Wykonawcą.** | SPEŁNIA  TAK /NIE |
|  | Zasilacz | Zewnętrzny, pracujący w sieci elektrycznej 230V 50/60Hz, max 90W. | SPEŁNIA  TAK /NIE |
|  | Obudowa waga i wymiary | Waga nie większa niż 1,8kg, grubość nie przekraczająca 20mm. Obudowa wzmocniona, szkielet wykonany ze wzmocnionego aluminium.  Obudowa musi spełniać standard MIL-STD 810G (potwierdzony w oficjalnych dokumentach producenta **lub wynikiem z przeprowadzonych testów - wymagane do załączenia na etapie umowy z Wykonawcą)** | SPEŁNIA  TAK /NIE |
|  | Bezpieczeństwo | - Zabezpieczenie BIOS hasłem użytkownika.  - Zabezpieczenie dysku twardego hasłem użytkownika.  - Złącze typu Kensington Lock.  - Zintegrowany z płytą główną dedykowany 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 - Trusted Platform Module 2.0. | SPEŁNIA  TAK /NIE |
|  | System operacyjny | Zainstalowany system operacyjny Windows 11 Professional lub równoważny  Parycja Recovery umożliwiająca w przypadku awarii dysku twardego ponowną instalację zainstalowanego systemu operacyjnego oraz nośnik zawierający sterowniki wszystkich zainstalowanych urządzeń  Windows 11 Professional lub równoważny:  System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego  3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim  4. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe  5. 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,  6. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.  7. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim  8. Wbudowany system pomocy w języku polskim.  9. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).  10. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące  11. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń  12. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń  13. Możliwość pracy w domenie Active Directory | **Producent**  **Nazwa i wersja oprogramowania**  SPEŁNIA  TAK /NIE |
|  | Certyfikaty i standardy | * Certyfikat ISO 9001, 14001, 50001 dla producenta sprzętu **(wymagany do załączenia na etapie umowy z Wykonawcą).** * Deklaracja zgodności CE i ROHS **(wymagany do załączenia na etapie umowy z Wykonawcą).** * Standard MIL-STD-810G (potwierdzony w oficjalnych dokumentach producenta **lub wynikiem z przeprowadzonych testów - wymagane do załączenia na etapie umowy z Wykonawcą)** | SPEŁNIA  TAK /NIE |
|  | Dodatkowe oprogramowanie zabezpieczające | System chroniący przed zagrożeniami, posiadający certyfikaty: OPSWAT Platinum, AV-Test ‘Top Product’, AV Comperative Advance +, ISO 27001 .  Szyfrowanie danych:  •Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.  •Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.  Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.  Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.  Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.  Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.  Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.  Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.  Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.  Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware  Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:  • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli  • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory  • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux  • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.  • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich  • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji  Zarządzanie przez Chmurę:  1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach  2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury  3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur  4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy  5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach  6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń  7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej  Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.  Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.  1.Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer  2.Oprogramowanie klienckie, zarządzane z poziomu serwera.  System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:  • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie  • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD  • funkcje regulowania połączeń WiFi i Bluetooth  • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe  • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi  • funkcje blokowania dostępu dowolnemu urządzeniu  • możliwość tymczasowego dodania dostępu do urządzenia przez administratora  • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu  • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka  • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora  • możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry  • możliwość używania tylko zaufanych urządzeń sieciowych,w tym urządzeń wskazanych na końcówkach klienckich  • funkcję wirtualnej klawiatury  • możliwość blokowania każdej aplikacji  • możliwość zablokowania aplikacji w oparciu o kategorie  • możliwość dodania własnych aplikacji do listy zablokowanych  • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze  • dodawanie innych aplikacji  • dodawanie aplikacji w formie portable  • możliwość wyboru pojedynczej aplikacji w konkretnej wersji  • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB  • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool  • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.  • możliwość zablokowania funkcji Printscreen  • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx  • funkcje monitorowania i kontroli przepływu poufnych informacji  • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików  • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj  • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe  • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe  • ochrona zawartości schowka systemu  • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL  • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych  • ochrona plików zamkniętych w archiwach  • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem  • możliwość tworzenia profilu DLP dla każdej polityki  • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania  • ochrona przez wyciekiem plików poprzez programy typu p2p  Monitorowanie zmian w plikach:  • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.  • Funkcje monitorowania określonych rodzajów plików.  • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.  • Generator raportów do funkcjonalności monitora zmian w plikach.  • możliwość śledzenia zmian we wszystkich plikach  • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach  • możliwość definiowana własnych typów plików  Optymalizacja systemu operacyjnego stacji klienckich:  • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku  • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem  • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich  • instruktaż stanowiskowy pracowników Zamawiającego  • dokumentacja techniczna w języku polskim  Wspierane platformy i systemy operacyjne:  1.Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)  2.Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)  3.Mac OS X, Mac OS 10  4.Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat  Platforma do zarządzania dla Android i iOS:  • Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę  • Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.  Zarządzanie użytkownikiem  • Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email  • Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika  • Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi  • Musi posiadać możliwość eksportu danych użytkownika  Zarządzanie urządzeniem  • Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO  • Musi umożliwiać import listy urządzeń z pliku CSV  • Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych  • Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta  • Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał  • Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres  • Musi zawierać podgląd aktualnie zainstalowanych aplikacji  • Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych,  • Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł  • Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres  Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:  Wymagania dotyczące technologii:  1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową  2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.  3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:  - Microsoft Internet Explorer  - Microsoft Edge  - Mozilla Firefox  - Google Chrome  - Safari  4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących  5 Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie  6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:  - Windows 2008 R2  - Windows 2012  - Windows 2012 R2  - Windows 2016  7. Portal zarządzający musi umożliwiać:  a) przegląd wybranych danych na podstawie konfigurowalnych widgetów  b) zablokowania możliwości zmiany konfiguracji widgetów  c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.  d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności  e) eksport wszystkich skanów podatności do pliku CSV  Backup i przywracanie danych  - Deduplikacja danych,  - Backup przyrostowy i różnicowy,  - Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,  - Backup danych lokalnych – plikowy oraz poczty Outlook,  - Backup otwartych plików (VSS),  - Filtr plików oraz folderów,  - Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),  - Wyłączanie komputera po wykonaniu backupu,  - Przywracanie danych do wskazanej lokalizacji,  - Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,  - Wyszukiwanie plików w repozytorium użytkownika,  Ustawienia  - Automatyczne logowanie,  - Zapamiętywanie danych logowania,  - Automatyczne uruchamianie programu przy starcie systemu,  - Ustawianie priorytetu dla procesu backupu,  - Zmiana klucza szyfrującego,  - Ustawienia przepustowości/zajętości pasma,  - Konfiguracja wydajności procesu backupu,  Bezpieczeństwo  - Zastępowanie nazwy pliku GUID-em,  - Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,  - Kompresja danych,  - Transmisja po bezpiecznym protokole TLS,  - Deklaracja klucza szyfrującego dane użytkownika,  - Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,  - Obliczanie sumy kontrolnej,  - Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski.  WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze, Mac OS,Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji.  Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. | **Producent**  **Nazwa i wersja oprogramowania**  SPEŁNIA  TAK /NIE |
|  | Wsparcie techniczne producenta | 1. Dostęp do aktualizacji systemu BIOS, podręczników użytkownika, najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta komputera numeru seryjnego lub modelu komputera – **do oferty należy dołączyć link strony poprzez wpisanie go w kolumnie obok.** 2. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu Komputera. 3. W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy zestawu oraz podzespoły montowane przez Producenta były przez niego certyfikowane. Wykonawca niebędący producentem oferowanego sprzętu nie może samodzielnie dokonywać jego modyfikacji. | **Podaj link strony** …………………….  SPEŁNIA  TAK /NIE |
|  | Dodatkowe oprogramowanie | Wykonawca dostarczy wraz z komputerem oprogramowanie producenta komputera które umożliwia aktualizację sterowników, pełne zarządzanie, monitoring, konfigurację a w szczególności: dystrybucję ustawień BIOS (zawierającego wcześniej zdefiniowane ustawienia jednakowe dla wszystkich), jednocześnie na wszystkich komputerach zgodnie z polityką bezpieczeństwa Zamawiającego.  Wykonawca dostarczy sterowniki w formacie dedykowanym dla Microsoft SCCM w celu dystrybucji za pomocą dołączonego oprogramowania producenta komputera zgodnie z polityką bezpieczeństwa Zamawiającego.  Zamawiający oczekuje oprogramowania zarządzającego produkowanego przez producenta i instalowanego przez producenta na etapie produkcji komputera. Program ma umożliwiać przynajmniej:  - monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów  - powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu  - powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów  - śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem.  Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające:   * upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, * 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 o:   + poprawkach i usprawnieniach dotyczących aktualizacji   + dacie wydania ostatniej aktualizacji | **Producent**  **Nazwa i wersja oprogramowania**  SPEŁNIA  TAK /NIE |
|  | Gwarancja | Gwarancja producenta komputera min. 36 miesięcy  Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta – wymagane oświadczenie potwierdzające, że serwis będzie realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego producenta (**oświadczenie wymagane do załączenia na etapie umowy z Wykonawcą).**  Autoryzowany Partner Serwisowy musi posiadać status autoryzowanego partnera serwisowego producenta komputera.  Serwis urządzeń musi być realizowany zgodnie z wymogami normy ISO9001  Wymagane okno czasowe dla zgłaszania usterek min. wszystkie dni robocze w godzinach od 8:00 do 20:00. Zgłoszenie serwisowe przyjmowane poprzez stronę www lub telefoniczne (dedykowany numer serwisowy do obsługi zgłoszeń serwisowych. | SPEŁNIA  TAK /NIE |

# Oprogramowanie biurowe – 2 licencje

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry (potwierdź spełnienie poprzez skreślenie niepoprawnej odpowiedzi) oraz wpis wymagane dane według wskazań** |
|  | Zastosowanie | Oprogramowanie będzie wykorzystywane do codziennych prac z wykorzystaniem edytora tekstu, arkusza kalkulacyjnego oraz pozostałych składników pakietu biurowego | **Producent**  **Nazwa i wersja oprogramowania** |
|  | Charakterystyka | Pakiet oprogramowania zawierającego minimum: edytor tekstu, arkusz kalkulacyjny, narzędzie do tworzenia prezentacji, narzędzie do tworzenia publikacji, klienta poczty MAPI w polskiej wersji językowej, wykonujące wszystkie funkcjonalności ww. pakietu oprogramowania biurowego, zapewniające możliwość instalacji i poprawnego działania na zaoferowanym systemie operacyjnym,  1.  Edytor tekstów umożliwiający:  a) Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty;  b) wstawianie oraz formatowanie tabel;  c)wstawianie oraz formatowanie obiektów graficznych;  d) wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele  przestawne);  e) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków;  f) automatyczne tworzenie spisów treści;  g) formatowanie nagłówków i stopek stron;  h) sprawdzanie pisowni w języku polskim; śledzenie zmian wprowadzonych przez użytkowników nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności;  j) określenie układu strony (pionowa/pozioma);  k) wydruk dokumentów; wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego  l) pracę na dokumentach utworzonych przy pomocy   oprogramowania Microsoft Word w wersjach 2003, 2007, 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu;  2. Arkusz kalkulacyjny umożliwiający:  a) Tworzenie raportów tabelarycznych; tworzenie wykresów liniowych (wraz z linią trendu), słupkowych, kołowych;  b) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu;  c) tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych;  d) wyszukiwanie i zamianę danych;  e) wykonywanie analiz danych przy użyciu formatowania warunkowego;  f) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie;  g) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności;  h) formatowanie czasu, daty i wartości finansowych z polskim formatem;  i) zapis wielu arkuszy kalkulacyjnych w jednym pliku; zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania zachowanie pełnej zgodności z formatami plików utworzonych za pomocą   oprogramowania Microsoft Excel w wersjach 2003, 2007, 2010, 2013 i 2016  3.Narzędzie do przygotowywania i prowadzenia prezentacji umożliwiające:  a) Przygotowywanie prezentacji multimedialnych, które będą:  -prezentowane przy użyciu projektora multimedialnego;  Licencja w wersji wieczystej. | SPEŁNIA  TAK /NIE |

# UPS do laptopów – 2 szt.

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  | Dane producenta | Podać dane producenta i model seria | **Producent:**  **Model wersja:** |
|  | Moc pozorna | min. 1500VA | SPEŁNIA  TAK /NIE |
|  | Moc rzeczywista | min. 900W | SPEŁNIA  TAK /NIE |
|  | Technologia | line-interactive | SPEŁNIA  TAK /NIE |
|  | Typ obudowy | tower | SPEŁNIA  TAK /NIE |
| **Wejście** | | | |
|  | Napięcie wejściowe | 220/230/240 VAC | SPEŁNIA  TAK /NIE |
|  | Zakres napięcia wejściowego | 140-300 VAC | SPEŁNIA  TAK /NIE |
| **Wyjście** | | | |
|  | Regulacja napięcia | +/- 10 % | SPEŁNIA  TAK /NIE |
|  | Regulacja Częstotliwości | 60 Hz lub 50 Hz ±1 Hz | SPEŁNIA  TAK /NIE |
|  | Kształt napięcia wyjściowego | symulowana sinusoida | SPEŁNIA  TAK /NIE |
|  | Typowy czas przełączania | 2-6 ms | SPEŁNIA  TAK /NIE |
| **Baterie** | | | |
|  | Baterie wewnętrzne w UPS | minimum 2x 12V 9Ah; szczelne, bezobsługowe | SPEŁNIA  TAK /NIE |
|  | Czas podtrzymania (dla 50% Pmax) | minimum 10 minut | SPEŁNIA  TAK /NIE |
| **Pozostałe** | | | |
|  | Wejście zasilania | kabel podłączony na stałe do UPSa | SPEŁNIA  TAK /NIE |
|  | Ilość i typ gniazd wyjściowych | minimum 4x Schuko (z podtrzymaniem) | SPEŁNIA  TAK /NIE |
|  | Stabilizacja napięcia AVR Boost & Buck | wymagana | SPEŁNIA  TAK /NIE |
|  | Filtr RJ45 | wymagany | SPEŁNIA  TAK /NIE |
|  | Ładowanie w trybie wyłączenia | wymagane | SPEŁNIA  TAK /NIE |
|  | Sygnalizacja | Dźwiękowa, Wyświetlacz LCD | SPEŁNIA  TAK /NIE |
|  | Alarmy dźwiękowe | minimum Tryb bateryjny, Rozładowana bateria, Przeciążenie, Awaria | SPEŁNIA  TAK /NIE |
|  | Funkcja autorestartu po powrocie zasilania | wymagana | SPEŁNIA  TAK /NIE |
|  | Funkcja zimnego startu | wymagana | SPEŁNIA  TAK /NIE |
|  | Informacje wyświetlane na panelu LCD | napięcie wejściowe, napięcie wyjściowe, poziom naładowania baterii, niski poziom naładowania baterii, poziom obciążenia, tryb sieciowy, tryb bateryjny | SPEŁNIA  TAK /NIE |
|  | Interfejs komunikacyjny | USB | SPEŁNIA  TAK /NIE |
|  | Zabezpieczenia | Minimum ochrona przed zwarciem, przeciążeniem, rozładowaniem | SPEŁNIA  TAK /NIE |
|  | Waga UPS | do 12 kg | SPEŁNIA  TAK /NIE |
|  | Wymiary UPS | nie większe niż: wysokość 205 mm; szerokość 146 mm, głębokość 398 mm | SPEŁNIA  TAK /NIE |
|  | Gwarancja | minimum 12 miesiące na elektronikę i 12 miesięcy na akumulatory; | SPEŁNIA  TAK /NIE |
|  | Serwis | autoryzowany serwis producenta zlokalizowany w Polsce. | SPEŁNIA  TAK /NIE |
| Naprawa maksymalnie 5 dni od daty zgłoszenia , w przypadku przekroczenia terminu Wykonawca dostarczy urządzenie zastępcze. **Na poświadczenie tego faktu, Wykonawca załączy Oświadczenie Producenta oferowanego sprzętu o spełnieniu tego wymogu - wymagane do załączenia na etapie umowy z Wykonawcą.** | SPEŁNIA  TAK /NIE |
| Naprawa w ramach gwarancji door-to-door | SPEŁNIA  TAK /NIE |
| Dystrybutor / Wykonawca ma Obowiązek na okres naprawy. Dostarczyć urządzenie zastępcze do siedziby Wykonawcy | SPEŁNIA  TAK /NIE |
|  | Oprogramowanie | oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS | SPEŁNIA  TAK /NIE |
| wsparcie dla systemów: Windows, Linux | SPEŁNIA  TAK /NIE |
| Oferent dostarczy jedno wspólne oprogramowanie do zarzadzania i monitorowania wszystkich proponowanych zasilaczy UPS. Oprogramowanie powinno być wskazane przez producenta zasilaczy UPS. Nie dopuszcza się możliwości dostosowywania oprogramowania innych producentów np. za pomocą skryptów. | SPEŁNIA  TAK /NIE |
| wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. | SPEŁNIA  TAK /NIE |
|  | Certyfikaty producenta | deklaracja zgodności CE **(wymagany do załączenia na etapie umowy z Wykonawcą)** | SPEŁNIA  TAK /NIE |
|  | Inne | Oferent powinien posiadać status Autoryzowanego Dystrybutora lub Autoryzowanego Partnera | SPEŁNIA  TAK /NIE |

…………………………………….

Data, czytelny podpis i pieczęć Oferenta