*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

**Załącznik Nr 1 do SWZ**

Opis przedmiotu zamówienia

(Znak postępowania: **ZPF.271.42.2022**)

Dotyczy zamówienia publicznego pn. Dostawa sprzętu i oprogramowania informatycznego w ramach grantu „Cyfrowa Gmina"

# Część 1

| Nazwa komponentu | Wymagane parametry techniczne |
|---|---|
| | **Stacje robocze (33 szt.)** |
| Typ | Komputer stacjonarny. |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. |
| Wydajność obliczeniowa | Procesor dedykowany do pracy w komputerach stacjonarnych.<br>Oferowany komputer musi osiągać w teście wydajności :<br>SYSMARK 25 Overall Rating – wynik min. 1500 pkt – **test z przeprowadzonej konfiguracji załączyć do oferty.**<br><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 Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia. |
| Pamięć RAM | Zainstalowane co najmniej 16 GB, możliwość rozbudowy do co najmniej 128 GB, co najmniej jeden wolny slot na moduły pamięci. |
| Pamięć masowa | Dysk SSD min. 500GB<br>Obudowa musi umożliwiać montaż dodatkowego dysku 2.5" lub 3.5". |
| Wydajność grafiki | Zintegrowana karta graficzna z procesorem osiągająca w teście Sysmark25 Creativity co najmniej 1400 punktów - **test z przeprowadzonej konfiguracji załączyć do oferty.** |
| Wyposażenie multimedialne | Karta dźwiękowa min. czterokanałowa zintegrowana z płytą główną, zgodna z High Definition. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. port audio line out. |
| Obudowa | Typu Small Form Factor z obsługą kart wyłącznie o niskim profilu. Umożliwiająca montaż 1 x dysku 3.5" lub 1 x dysku 2.5" wewnątrz obudowy. Napęd optyczny zamontowany w dedykowanej wnęce zewnętrznej 5.25" typu slim. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Suma wymiarów obudowy nieprzekraczająca 78 cm.<br>Na panelu przednim zamontowany filtr powietrza chroniący wnętrze przed kurzem, pyłem itp. Filtr demontowany bez użycia narzędzi.<br>Zasilacz o mocy min. 300W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 92% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 89% przy obciążeniu zasilacza na poziomie 100%,<br>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). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS'u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. |
| Bezpieczeństwo | Ukryty w laminacie płyty głównej 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. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego |

| | |
|---|---|
| | uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność. |
| BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy.<br>BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio.<br>Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie.<br>Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT" (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo.<br>Możliwość dokonywania backup'u BIOS wraz z ustawieniami na dysku wewnętrznym. Funkcja włączająca przypomnienie o konieczności oczyszczenia lub zastąpienia filtra powietrza w jednej z opcji dostępnych : co 15 dni, co 30 dni, co 60 dni, co 90 dni, co 120 dni, co 150 dni i co 180dni<br>Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot'owania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS. |
| Wirtualizacja | Sprzętowe wsparcie technologi wirtualizacji realizowane łącznie w procesorze, chipsecie płyty główej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). |
| System operacyjny | Zainstalowany system operacyjny Windows 11 Professional lub równoważny, klucz licencyjny musi umożliwiać instalację systemu operacyjnego zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego. |
| Oprogramowanie zabezpieczające | System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej:<br>• wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,<br>• wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik |

| | |
|---|---|
| | behawioralnych,<br>• wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)<br>Szyfrowanie danych:<br>• 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 lub równoważnym.<br>• 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.<br>Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.<br>Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.<br>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.<br>Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.<br>Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.<br>Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.<br>Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną anyransomware.<br>Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware.<br>Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:<br>• Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows lub równoważnych), w formie plików .exe lub .msi dla Windows lub równoważnych oraz formatach dla systemów Linux<br>• 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.<br>• 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<br>• Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji<br>Zarządzanie przez Chmurę:<br>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<br>3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur<br>4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy<br>5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach<br>6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń<br>7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej<br><br>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.<br>Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.<br>1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer<br>2. Oprogramowanie klienckie, zarządzane z poziomu serwera.<br>System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:<br>• różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie<br>• funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD<br>• funkcje regulowania połączeń WiFi i Bluetooth<br>• funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe<br>• funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi<br>• funkcje blokowania dostępu dowolnemu urządzeniu<br>• możliwość tymczasowego dodania dostępu do urządzenia przez administratora<br>• zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu<br>• możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka<br>• możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora<br>• możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich<br>• funkcję wirtualnej klawiatury<br>• możliwość blokowania każdej aplikacji<br>• możliwość zablokowania aplikacji w oparciu o kategorie<br>• możliwość dodania własnych aplikacji do listy zablokowanych<br>• zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze<br>• dodawanie innych aplikacji<br>• dodawanie aplikacji w formie portable<br>• możliwość wyboru pojedynczej aplikacji w konkretnej wersji |

| | |
|---|---|
| | • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB<br>• kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool<br>• możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.<br>• możliwość zablokowania funkcji Printscreen<br>• funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows lub równoważnym jak i OSx<br>• funkcje monitorowania i kontroli przepływu poufnych informacji<br>• możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików<br>• możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj<br>• możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe<br>• ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe<br>• ochrona zawartości schowka systemu<br>• ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL<br>• możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych<br>• ochrona plików zamkniętych w archiwach<br>• Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem<br>• możliwość tworzenia profilu DLP dla każdej polityki<br>• wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania<br>• ochrona przez wyciekiem plików poprzez programy typu p2p<br>Monitorowanie zmian w plikach:<br>• Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.<br>• Funkcje monitorowania określonych rodzajów plików.<br>• Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.<br>• Generator raportów do funkcjonalności monitora zmian w plikach.<br>• możliwość śledzenia zmian we wszystkich plikach<br>• możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach<br>• możliwość definiowana własnych typów plików<br>Optymalizacja systemu operacyjnego stacji klienckich:<br>• usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku<br>• optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem<br>• możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich<br>• instruktaż stanowiskowy pracowników Zamawiającego<br>• dokumentacja techniczna w języku polskim<br><br>Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa: |

| | |
|---|---|
| | Wymagania dotyczące technologii:<br>1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową<br>2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.<br>3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:<br>- Microsoft Internet Explorer<br>- Microsoft Edge<br>- Mozilla Firefox<br>- Google Chrome<br>- Safari<br>4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących<br>5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie<br>6. Portal zarządzający musi umożliwiać:<br>a) przegląd wybranych danych na podstawie konfigurowalnych widgetów<br>b) zablokowania możliwości zmiany konfiguracji widgetów<br>c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.<br>d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności<br>e) eksport wszystkich skanów podatności do pliku CSV<br><br>Backup i przywracanie danych<br>- Deduplikacja danych na źródle,<br>- Backup przyrostowy i różnicowy,<br>- Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,<br>- Backup danych lokalnych – plikowy oraz poczty Outlook,<br>- Backup otwartych plików (VSS),<br>- Filtr plików oraz folderów,<br>- Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),<br>- Wyłączanie komputera po wykonaniu backupu,<br>- Przywracanie danych do wskazanej lokalizacji,<br>- Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,<br>- Wyszukiwanie plików w repozytorium użytkownika,<br>Ustawienia<br>- Automatyczne logowanie,<br>- Zapamiętywanie danych logowania,<br>- Automatyczne uruchamianie programu przy starcie systemu,<br>- Ustawianie priorytetu dla procesu backupu, |

| | |
|---|---|
| | - Zmiana klucza szyfrującego,<br>- Ustawienia przepustowości/zajętości pasma,<br>- Konfiguracja wydajności procesu backupu,<br>Bezpieczeństwo<br>- Zastępowanie nazwy pliku GUID-em,<br>- Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,<br>- Kompresja danych,<br>- Transmisja po bezpiecznym protokole TLS,<br>- Deklaracja klucza szyfrującego dane użytkownika,<br>- Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,<br>- Obliczanie sumy kontrolnej,<br>- Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski.<br>WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze lub równoważnym 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. |
| Certyfikaty i standardy | Deklaracja zgodności CE lub równoważne<br>Urządzenia muszą być wyprodukowane zgodnie z normą ISO 50001 oraz ISO 9001.<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. |
| Wymagania dodatkowe | Wbudowane porty: 1x HDMI 1.4, 1x VGA, 2x DisplayPort, port audio combo (słuchawka/mikrofon) na przednim panelu panelu, 1xRJ-45, Wbudowany czytnik kart pamięci SD.<br>9 portów USB wyprowadzonych na zewnątrz obudowy, w układzie:<br>- Panel przedni: 5x USB 3.2, w tym 1x USB-C<br>- Panel tylny: 4x USB Typu A<br>Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej.<br>Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika),<br>Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia, wyposażona w:<br>2x PCIe x16 Gen.3,<br>1x PCIe x1,<br>1x PCI |

| | |
|---|---|
| | 4x DIMM z obsługą do 128 GB, 2x SATA w tym min. 1 szt SATA 3.0.<br>Jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej.<br>Klawiatura USB w układzie polski programisty<br>Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll)<br>Wbudowana nagrywarka DVD +/-RW |
| Wsparcie techniczne producenta | Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego). |
| Dodatkowe oprogramowanie | Oprogramowanie zarządzające producenta komputera, instalowane na etapie produkcji komputera, umożliwiające min.:<br>- powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu<br>- powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów<br>Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające:<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 o:<br>poprawkach i usprawnieniach dotyczących aktualizacji<br>dacie wydania ostatniej aktualizacji<br>priorytecie aktualizacji<br>zgodności z systemami operacyjnymi<br>jakiego komponentu sprzętu dotyczy aktualizacja<br>wszystkich poprzednich aktualizacjach z informacjami jak powyżej.<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. |
| Oprogramowanie pakietu biurowego | Oferowane stacje robocze (UWAGA! Dotyczy 33 szt.,) muszą zostać dostarczone z bezterminową licencją oprogramowania pakietu biurowego klasy Microsoft Office 2021 umożliwiającego pracę z edytorem tekstów i arkuszem kalkulacyjnym oraz posiadający narzędzie do przygotowania i prowadzenia prezentacji wraz z narzędziem do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) lub równoważny.<br><br>Za równoważny system pakietu biurowego Zamawiający uzna system spełniający następujące minimalne parametry:<br><br>a. Dostawa pełnej polskiej wersji językowej interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. Pakiet powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim. Dostępność w Internecie na stronach producenta biuletynów |

| | |
|---|---|
| | technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach pracy Urzędu – cena połączenia nie większa niż cena połączenia lokalnego. Publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej trzy lata od daty zakupu. Możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0).<br>b. Zintegrowany pakiet aplikacji biurowych musi zawierać co najmniej:<br>• edytor tekstów,<br>• arkusz kalkulacyjny,<br>• narzędzie do przygotowania i prowadzenia prezentacji,<br>• narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).<br>c. Edytor tekstów musi umożliwiać co najmniej:<br>• 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.<br>• Wstawianie oraz formatowanie tabel.<br>• Wstawianie oraz formatowanie obiektów graficznych.<br>• Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).<br>• Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.<br>• Automatyczne tworzenie spisów treści.<br>• Formatowanie nagłówków i stopek stron.<br>• Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.<br>• Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.<br>• Określenie układu strony (pionowa/pozioma).<br>• Wydruk dokumentów.<br>• Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.<br>• Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.<br>• Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.<br>d. Arkusz kalkulacyjny musi umożliwiać co najmniej:<br>• Tworzenie raportów tabelarycznych.<br>• Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.<br>• Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.<br>• Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, |

| | |
|---|---|
| | pliki XML, webservice).<br>• Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych.<br>• Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.<br>• Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.<br>• Wyszukiwanie i zamianę danych.<br>• Wykonywanie analiz danych przy użyciu formatowania warunkowego.<br>• Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.<br>• Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.<br>• Formatowanie czasu, daty i wartości finansowych z polskim formatem.<br>• Zapis wielu arkuszy kalkulacyjnych w jednym pliku.<br>• Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.<br>e. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać co najmniej:<br>• Przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego.<br>• Drukowanie w formacie umożliwiającym robienie notatek.<br>• Zapisanie jako prezentacja tylko do odczytu.<br>• Nagrywanie narracji i dołączanie jej do prezentacji.<br>• Opatrywanie slajdów notatkami dla prezentera.<br>• Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.<br>• Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.<br>• Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.<br>• Możliwość tworzenia animacji obiektów i całych slajdów.<br>• Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.<br>f. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:<br>• Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.<br>• Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.<br>• Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.<br>• Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.<br>• Automatyczne grupowanie poczty o tym samym tytule.<br>• Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.<br>• Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.<br>• Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.<br>• Zarządzanie kalendarzem. |

| | |
|---|---|
| | • Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.<br>• Przeglądanie kalendarza innych użytkowników.<br>• Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.<br>• Zarządzanie listą zadań.<br>• Zlecanie zadań innym użytkownikom.<br>• Zarządzanie listą kontaktów.<br>• Udostępnianie listy kontaktów innym użytkownikom.<br>• Przeglądanie listy kontaktów innych użytkowników.<br>Możliwość przesyłania kontaktów innym użytkowników. |
| Monitor (parametry minimalne) | Typ ekranu: Ekran ciekłokrystaliczny z aktywną matrycą min. 23,8” (16:9) |
| Monitor (parametry minimalne) | Technologia wykonania matrycy: IPS |
| Monitor (parametry minimalne) | Rozmiar plamki: Maksymalnie 0,275mm |
| Monitor (parametry minimalne) | Jasność: Min. 250 cd/m2 |
| Monitor (parametry minimalne) | Kontrast: Min. 1000:1 |
| Monitor (parametry minimalne) | Kąty widzenia (pion/poziom): 178/178 stopni |
| Monitor (parametry minimalne) | Czas reakcji matrycy: max. 8 ms |
| Monitor (parametry minimalne) | Rozdzielczość maksymalna: Min. 1920 x 1080 przy 60Hz |
| Monitor (parametry minimalne) | Paleta kolorów: 83% (CIE 1976) |

| | |
|---|---|
| Monitor (parametry minimalne) | Głębia kolorów: 16,7 miliona kolorów |
| Monitor (parametry minimalne) | Zużycie energii : Maks. 28W<br>W trybie uśpienia maks. 0,3W |
| Monitor (parametry minimalne) | Powłoka powierzchni ekranu: Antyodblaskowa utwardzona |
| Monitor (parametry minimalne) | Podświetlenie: System podświetlenia LED |
| Monitor (parametry minimalne) | Bezpieczeństwo: Monitor musi być wyposażony w tzw. gniazdo zabezpieczenia przed kradzieżą.<br>Wbudowane w monitor narzędzie diagnostyczne umożliwiające<br>zdiagnozowanie problemu wyświetlania obrazu na ekranie. |
| Monitor (parametry minimalne) | Pochylenie monitora:<br>W zakresie min. 26 stopni.<br>Regulacja wysokości min. 100mm |
| Monitor (parametry minimalne) | Kolor obudowy Czarny |
| Monitor (parametry minimalne) | Złącze:<br>1 x D-Sub<br>1 x DisplayPort 1.2<br>1 x HDMI 1.4 |
| Gwarancja | Gwarancja: min. 24 miesiące gwarancji producenta świadczona na miejscu u użytkownika końcowego na cały zestaw komputerowy, możliwość zgłaszania awarii przez ogólnopolską linię telefoniczną i<br>stronę internetową producenta.<br>Czas reakcji serwisu - do końca następnego dnia roboczego<br>Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług<br>serwisowych oraz posiadać autoryzacje producenta. |

| **Laptop TYP A (15 szt.)** | |
|---|---|
| Komputer | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. |
| Ekran | Matryca IPS, min. 17,3" z podświetleniem w technologii LED, rozdzielczość co najmniej: 1920x1080 (FHD), 220nits |
| Obudowa | Obudowa komputera matowa, zawiasy metalowe. Kąt otwarcia matrycy min.140 stopni. W obudowe wbudowane co najmien 2 diody sygnalizujące stan naładowania akumulatora oraz pracę dysku twardego. |
| Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejs SATA III (6 Gb/s) do obsługi dysków twardych. |
| Wydajność komputera | Oferowany komputer przenośny musi osiągać w teście wydajności :<br>SYSMARK 25 – wynik min. 1200.<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 Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia. |
| Pamięć operacyjna | Min 16GB z możliwością rozbudowy do 32GB. |
| Dysk twardy | Min. 512GB SSD 2.5 lub M2 zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |
| Karta graficzna | Zintegrowana karta graficzna z min. 2GB pamięci dynamicznej. Osiągająca w teście Sysmark25 Creativity min. 1000 pkt. - **test z przeprowadzonej konfiguracji załączyć do oferty.** |
| Audio/Video | Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo min 2x 2W, wbudowany mikrofon, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute), kamera HD720p |

| | |
|---|---|
| Porty/złącza | 3xUSB w tym min. 1x USB 3.2 typ-C oraz 1x USB 3.2 typ-A, złącze słuchawek i złącze mikrofonu typu COMBO, 1xHDMI. |
| Klawiatura | Klawiatura wyspowa, układ US. |
| WiFi | Wbudowana karta sieciowa, pracująca w standardzie AC |
| Bluetooth | Wbudowany moduł Bluetooth 4.1 |
| Bateria | Bateria pozwalająca na nieprzerwaną pracę urządzenia min. 6 godzin - wynik z przeprowadzonego testu MobileMark Battery Life – **test z przeprowadzonej konfiguracji załączyć do oferty.** |
| Zasilacz | Zasilacz zewnętrzny max 65W |
| BIOS | BIOS zgodny ze specyfikacją UEFI.<br>Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji:<br>- wersji BIOS<br>- nr seryjnym komputera<br>- ilości pamięci RAM<br>- typie procesora i jego prędkości<br>- modele zainstalowanych dysków twardych<br>Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynnośći:<br>Możliwość ustawienia hasła dla twardego dysku<br>Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password<br>Możliwość ustawienia hasła Administratora i użytkowanika BIOS<br>Mozliwość włączania/wyłaczania wirutalizacji z poziomu BIOSU<br>Możliwość Wyłączania/Włączania: zintegrowanej karty WIFI, portów USB, Tryby PXE dla karty sieciowej,<br>Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. |
| Bezpieczeństwo | - złącze Kensington Lock,<br>- 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 (TPM 2.0). |
| Certyfikaty i standardy | Certyfikat ISO9001:2000 dla producenta sprzętu<br>Deklaracja zgodności CE |

| | |
|---|---|
| | Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki. |
| System operacyjny | Windows 11 Professional 64 bit lub równoważny:<br>System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:<br>Dostępne dwa rodzaje graficznego interfejsu użytkownika:<br>Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,<br>Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych<br>Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego<br>Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim<br>Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.<br>Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe<br>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>Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.<br>Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim<br>Wbudowany system pomocy w języku polskim.<br>Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).<br>Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. |
| Oprogramowanie zabezpieczające | System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej:<br>• wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,<br>• wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,<br>• wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)<br>Szyfrowanie danych:<br>• 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 lub równoważnym,<br>• 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.<br>Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.<br>Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.<br>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.<br>Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.<br>Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.<br>Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.<br>Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną anyransomware.<br>Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware.<br>Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:<br>• Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows lub równoważnym), w formie plików .exe lub .msi dla Windows lub równoważnego<br>• 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.<br>• 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<br>• Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji<br>Zarządzanie przez Chmurę:<br>1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach<br>2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury<br>3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur<br>4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy<br>5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach |

| | |
|---|---|
| | 6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń<br>7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej<br><br>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.<br>Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.<br>1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer<br>2. Oprogramowanie klienckie, zarządzane z poziomu serwera.<br>System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:<br>• różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie<br>• funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD<br>• funkcje regulowania połączeń WiFi i Bluetooth<br>• funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe<br>• funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi<br>• funkcje blokowania dostępu dowolnemu urządzeniu<br>• możliwość tymczasowego dodania dostępu do urządzenia przez administratora<br>• zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu<br>• możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka<br>• możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora<br>• możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich<br>• funkcję wirtualnej klawiatury<br>• możliwość blokowania każdej aplikacji<br>• możliwość zablokowania aplikacji w oparciu o kategorie<br>• możliwość dodania własnych aplikacji do listy zablokowanych<br>• zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze<br>• dodawanie innych aplikacji<br>• dodawanie aplikacji w formie portable<br>• możliwość wyboru pojedynczej aplikacji w konkretnej wersji<br>• dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB<br>• kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool<br>• możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.<br>• możliwość zablokowania funkcji Printscreen |

| | |
|---|---|
| | • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows lub równoważnym jak i OSx<br>• funkcje monitorowania i kontroli przepływu poufnych informacji<br>• możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików<br>• możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj<br>• możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe<br>• ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe<br>• ochrona zawartości schowka systemu<br>• ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL<br>• możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych<br>• ochrona plików zamkniętych w archiwach<br>• Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem<br>• możliwość tworzenia profilu DLP dla każdej polityki<br>• wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania<br>• ochrona przez wyciekiem plików poprzez programy typu p2p<br>Monitorowanie zmian w plikach:<br>• Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.<br>• Funkcje monitorowania określonych rodzajów plików.<br>• Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.<br>• Generator raportów do funkcjonalności monitora zmian w plikach.<br>• możliwość śledzenia zmian we wszystkich plikach<br>• możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach<br>• możliwość definiowana własnych typów plików<br>Optymalizacja systemu operacyjnego stacji klienckich:<br>• usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku<br>• optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem<br>• możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich<br>• instruktaż stanowiskowy pracowników Zamawiającego<br>• dokumentacja techniczna w języku polskim<br><br>Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:<br>Wymagania dotyczące technologii:<br>1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową<br>2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.<br>3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:<br>- Microsoft Internet Explorer |

| | |
|---|---|
| | - Microsoft Edge<br>- Mozilla Firefox<br>- Google Chrome<br>- Safari<br>4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących<br>5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie<br>6. Portal zarządzający musi umożliwiać:<br>a) przegląd wybranych danych na podstawie konfigurowalnych widgetów<br>b) zablokowania możliwości zmiany konfiguracji widgetów<br>c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.<br>d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności<br>e) eksport wszystkich skanów podatności do pliku CSV<br><br>Backup i przywracanie danych<br>- Deduplikacja danych,<br>- Backup przyrostowy i różnicowy,<br>- Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,<br>- Backup danych lokalnych – plikowy oraz poczty Outlook,<br>- Backup otwartych plików (VSS),<br>- Filtr plików oraz folderów,<br>- Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),<br>- Wyłączanie komputera po wykonaniu backupu,<br>- Przywracanie danych do wskazanej lokalizacji,<br>- Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,<br>- Wyszukiwanie plików w repozytorium użytkownika,<br>Ustawienia<br>- Automatyczne logowanie,<br>- Zapamiętywanie danych logowania,<br>- Automatyczne uruchamianie programu przy starcie systemu,<br>- Ustawianie priorytetu dla procesu backupu,<br>- Zmiana klucza szyfrującego,<br>- Ustawienia przepustowości/zajętości pasma,<br>- Konfiguracja wydajności procesu backupu,<br>Bezpieczeństwo<br>- Zastępowanie nazwy pliku GUID-em, |

| | |
|---|---|
| | - Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,<br>- Kompresja danych,<br>- Transmisja po bezpiecznym protokole TLS,<br>- Deklaracja klucza szyfrującego dane użytkownika,<br>- Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,<br>- Obliczanie sumy kontrolnej,<br>- Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski.<br>WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze lub równoważnym 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. |
| Gwarancja | Min. 24 miesiące gwarancji, czas reakcji serwisu, do końca następnego dnia roboczego. Gwarancja musi musi oferować przez cały okres :<br>- mieć opiekę kierownika technicznego ds. Eskalacji<br>- dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu przez cały rok (w języku polskim w dni robocze)<br>Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. |
| Wsparcie techniczne producenta | Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej.<br>- możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego<br>- Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |
| Oprogramowanie pakietu biurowego | Oferowane laptopy (UWAGA! Dotyczy 15 szt.,) muszą zostać dostarczone z bezterminową licencją oprogramowania pakietu biurowego klasy Microsoft Office 2021 umożliwiającego pracę z edytorem tekstów i arkuszem kalkulacyjnym oraz posiadający narzędzie do przygotowania i prowadzenia prezentacji wraz z narzędziem do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) lub równoważny.<br><br>Za równoważny system pakietu biurowego Zamawiający uzna system spełniający następujące minimalne parametry:<br><br>a. Dostawa pełnej polskiej wersji językowej interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. Pakiet powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim. Dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach pracy Urzędu – cena połączenia nie większa niż cena połączenia lokalnego. Publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej trzy lata od daty zakupu. Możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0). |

| | |
|---|---|
| | b. Zintegrowany pakiet aplikacji biurowych musi zawierać co najmniej:<br>• edytor tekstów,<br>• arkusz kalkulacyjny,<br>• narzędzie do przygotowania i prowadzenia prezentacji,<br>• narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).<br>c. Edytor tekstów musi umożliwiać co najmniej:<br>• 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.<br>• Wstawianie oraz formatowanie tabel.<br>• Wstawianie oraz formatowanie obiektów graficznych.<br>• Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).<br>• Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.<br>• Automatyczne tworzenie spisów treści.<br>• Formatowanie nagłówków i stopek stron.<br>• Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.<br>• Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.<br>• Określenie układu strony (pionowa/pozioma).<br>• Wydruk dokumentów.<br>• Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.<br>• Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.<br>• Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.<br>d. Arkusz kalkulacyjny musi umożliwiać co najmniej:<br>• Tworzenie raportów tabelarycznych.<br>• Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.<br>• Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.<br>• Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice).<br>• Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych.<br>• Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.<br>• Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. |

| | |
|---|---|
| | • Wyszukiwanie i zamianę danych.<br>• Wykonywanie analiz danych przy użyciu formatowania warunkowego.<br>• Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.<br>• Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.<br>• Formatowanie czasu, daty i wartości finansowych z polskim formatem.<br>• Zapis wielu arkuszy kalkulacyjnych w jednym pliku.<br>• Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.<br>e. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać co najmniej:<br>• Przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego.<br>• Drukowanie w formacie umożliwiającym robienie notatek.<br>• Zapisanie jako prezentacja tylko do odczytu.<br>• Nagrywanie narracji i dołączanie jej do prezentacji.<br>• Opatrywanie slajdów notatkami dla prezentera.<br>• Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.<br>• Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.<br>• Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.<br>• Możliwość tworzenia animacji obiektów i całych slajdów.<br>• Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.<br>f. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:<br>• Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.<br>• Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.<br>• Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.<br>• Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.<br>• Automatyczne grupowanie poczty o tym samym tytule.<br>• Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.<br>• Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.<br>• Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.<br>• Zarządzanie kalendarzem.<br>• Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.<br>• Przeglądanie kalendarza innych użytkowników.<br>• Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.<br>• Zarządzanie listą zadań.<br>• Zlecanie zadań innym użytkownikom. |

| | |
|---|---|
| | • Zarządzanie listą kontaktów.<br>• Udostępnianie listy kontaktów innym użytkownikom.<br>• Przeglądanie listy kontaktów innych użytkowników.<br>Możliwość przesyłania kontaktów innym użytkowników. |
| **Laptop TYP B (2 szt.)** | |
| Komputer | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. |
| Ekran | Matryca matowa IPS, min. 17,3" z podświetleniem w technologii LED, rozdzielczość: min. 1920x1080, jasność matrycy min. 250 cd/m2. Matryca z pokryciem barw 100% sRGB. |
| Obudowa | Obudowa komputera matowa, zawiasy metalowe. Kąt otwarcia matrycy min.140 stopni. W obudowe wbudowane co najmien 2 diody sygnalizujące stan naładowania akumulatora oraz pracę dysku twardego. Aluminiowa pokrywa matrycy. Obudowa posiadająca czujnik temperatury dostosowujący pracę wentylatorów. |
| Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejs SATA III (6 Gb/s) do obsługi dysków twardych. |
| Wydajność komputera | Oferowany komputer przenośny musi osiągać w teście wydajności :<br>SYSMARK 25 – wynik min. 1500.<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 Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia wraz z ofertą. |
| Pamięć operacyjna | Min. 32GB, rodzaj pamięci (nie dopuszcza się wlutowanych pamięci w płytę główną). |
| Dysk twardy | Min. 500GB SSD zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |
| Karta graficzna | Niezintegrowana karta graficzna z pamięcią min. 4 GB. Osiągająca w teście Sysmark25 Creativity min. 1300 pkt. –n **test z przeprowadzonej konfiguracji załączyć do oferty.** |

| | |
|---|---|
| | |
| Audio/Video | Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo min 2x 2W, wbudowany mikrofon, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute), kamera HD720p. Wbudowany wyłącznik kamery. |
| Porty/złącza | 3xUSB 3.2 oraz min. 1x USB 3.2 typ-C, złącze słuchawek i złącze mikrofonu typu COMBO, 1xHDMI 2.0, 1x RJ45 (1Gb/s). |
| Klawiatura | Klawiatura wyspowa, układ US. Klawiatura z wbudowanym podświetleniem. Wydzielony układ numeryczny po prawej stronie. |
| WiFi | Wbudowana karta sieciowa, pracująca w standardzie AX |
| Bluetooth | Wbudowany moduł Bluetooth 5.2 |
| Bateria | Bateria pozwalająca na nieprzerwaną pracę urządzenia min. 6 godzin - wynik z przeprowadzonego testu MobileMark 25 Battery Life. |
| Zasilacz | Zasilacz zewnętrzny min. 120W |
| BIOS | BIOS zgodny ze specyfikacją UEFI.<br>Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji:<br>- wersji BIOS<br>- nr seryjnym komputera<br>- ilości pamięci RAM<br>- typie procesora i jego prędkości<br>-modele zainstalowanych dysków twardych<br>Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynnośći:<br>Możliwość ustawienia hasła dla twardego dysku<br>Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password<br>Możliwość ustawienia hasła Administratora i użytkowanika BIOS<br>Mozliwość włączania/wyłaczania wirutalizacji z poziomu BIOSU<br>Możliwość Wyłączania/Włączania: zintegrowanej karty WIFI, portów USB, Tryby PXE dla karty sieciowej,<br>Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu |

| | |
|---|---|
| | USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. |
| Bezpieczeństwo | 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 (TPM 2.0). |
| Certyfikaty i standardy | Certyfikat ISO9001, 50001 dla producenta sprzętu<br>Deklaracja zgodności CE<br>Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki |
| System operacyjny | Windows 11 Professional 64 bit lub równoważny:<br>System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:<br>Dostępne dwa rodzaje graficznego interfejsu użytkownika:<br>Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,<br>Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych<br>Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego<br>Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim<br>Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.<br>Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe<br>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>Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.<br>Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim<br>Wbudowany system pomocy w języku polskim.<br>Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).<br>Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. |
| Bezpieczeństwo i oprogramowanie | System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej: |

| | |
|---|---|
| dodatkowe | • wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,<br>• wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,<br>• wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)<br>Szyfrowanie danych:<br>• 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 lub równoważnym.<br>• 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.<br>Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.<br>Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.<br>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.<br>Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.<br>Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.<br>Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.<br>Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną anyransomware.<br>Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware.<br>Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:<br>• Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows lub równoważnych), w formie plików .exe lub .msi dla Windows lub równoważnego<br>• 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.<br>• 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<br>• Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji<br>Zarządzanie przez Chmurę: |

| | |
|---|---|
| | 1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach<br>2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury<br>3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur<br>4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy<br>5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach<br>6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń<br>7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej<br><br>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.<br>Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.<br>1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer<br>2. Oprogramowanie klienckie, zarządzane z poziomu serwera.<br>System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:<br>• różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie<br>• funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD<br>• funkcje regulowania połączeń WiFi i Bluetooth<br>• funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe<br>• funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi<br>• funkcje blokowania dostępu dowolnemu urządzeniu<br>• możliwość tymczasowego dodania dostępu do urządzenia przez administratora<br>• zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu<br>• możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka<br>• możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora<br>• możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich<br>• funkcję wirtualnej klawiatury<br>• możliwość blokowania każdej aplikacji<br>• możliwość zablokowania aplikacji w oparciu o kategorie<br>• możliwość dodania własnych aplikacji do listy zablokowanych<br>• zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze<br>• dodawanie innych aplikacji |

| | |
|---|---|
| | • dodawanie aplikacji w formie portable<br>• możliwość wyboru pojedynczej aplikacji w konkretnej wersji<br>• dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB<br>• kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool<br>• możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.<br>• możliwość zablokowania funkcji Printscreen<br>• funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows lub równoważnym jak i OSx<br>• funkcje monitorowania i kontroli przepływu poufnych informacji<br>• możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików<br>• możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj<br>• możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe<br>• ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe<br>• ochrona zawartości schowka systemu<br>• ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL<br>• możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych<br>• ochrona plików zamkniętych w archiwach<br>• Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem<br>• możliwość tworzenia profilu DLP dla każdej polityki<br>• wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania<br>• ochrona przez wyciekiem plików poprzez programy typu p2p<br>Monitorowanie zmian w plikach:<br>• Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.<br>• Funkcje monitorowania określonych rodzajów plików.<br>• Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.<br>• Generator raportów do funkcjonalności monitora zmian w plikach.<br>• możliwość śledzenia zmian we wszystkich plikach<br>• możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach<br>• możliwość definiowana własnych typów plików<br>Optymalizacja systemu operacyjnego stacji klienckich:<br>• usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku<br>• optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem<br>• możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich<br>• instruktaż stanowiskowy pracowników Zamawiającego<br>• dokumentacja techniczna w języku polskim |

| | |
|---|---|
| | Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:<br>Wymagania dotyczące technologii:<br>1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową<br>2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.<br>3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:<br>- Microsoft Internet Explorer<br>- Microsoft Edge<br>- Mozilla Firefox<br>- Google Chrome<br>- Safari<br>4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących<br>5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie<br>6. Portal zarządzający musi umożliwiać:<br>a) przegląd wybranych danych na podstawie konfigurowalnych widgetów<br>b) zablokowania możliwości zmiany konfiguracji widgetów<br>c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.<br>d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności<br>e) eksport wszystkich skanów podatności do pliku CSV<br><br>Backup i przywracanie danych<br>- Deduplikacja danych na źródle,<br>- Backup przyrostowy i różnicowy,<br>- Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,<br>- Backup danych lokalnych – plikowy oraz poczty Outlook,<br>- Backup otwartych plików (VSS),<br>- Filtr plików oraz folderów,<br>- Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),<br>- Wyłączanie komputera po wykonaniu backupu,<br>- Przywracanie danych do wskazanej lokalizacji,<br>- Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,<br>- Wyszukiwanie plików w repozytorium użytkownika,<br>Ustawienia<br>- Automatyczne logowanie,<br>- Zapamiętywanie danych logowania, |

| | |
|---|---|
| | - Automatyczne uruchamianie programu przy starcie systemu,<br>- Ustawianie priorytetu dla procesu backupu,<br>- Zmiana klucza szyfrującego,<br>- Ustawienia przepustowości/zajętości pasma,<br>- Konfiguracja wydajności procesu backupu,<br>Bezpieczeństwo<br>- Zastępowanie nazwy pliku GUID-em,<br>- Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,<br>- Kompresja danych,<br>- Transmisja po bezpiecznym protokole TLS,<br>- Deklaracja klucza szyfrującego dane użytkownika,<br>- Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,<br>- Obliczanie sumy kontrolnej,<br>- Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski.<br>WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze lub równoważne 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. |
| Gwarancja | Min . 24 miesiące gwarancji, czas reakcji serwisu, do końca następnego dnia roboczego. Gwarancja musi musi oferować przez cały okres :<br>- mieć opiekę kierownika technicznego ds. Eskalacji<br>- dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu przez cały rok (w języku polskim w dni robocze)<br>Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. |
| Wsparcie techniczne producenta | Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej.<br>- możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego<br>- Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |
| Oprogramowanie pakietu biurowego | Oferowane laptopy (UWAGA! Dotyczy 2 szt.,) muszą zostać dostarczone z bezterminową licencją oprogramowania pakietu biurowego klasy Microsoft Office 2021 umożliwiającego pracę z edytorem tekstów i arkuszem kalkulacyjnym oraz posiadający narzędzie do przygotowania i prowadzenia prezentacji wraz z narzędziem do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) lub równoważny.<br>Za równoważny system pakietu biurowego Zamawiający uzna system spełniający następujące minimalne parametry:<br>a. Dostawa pełnej polskiej wersji językowej interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku |

| | |
|---|---|
| | polskim. Pakiet powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim. Dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach pracy Urzędu – cena połączenia nie większa niż cena połączenia lokalnego. Publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej trzy lata od daty zakupu. Możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0).<br><br>b. Zintegrowany pakiet aplikacji biurowych musi zawierać co najmniej:<br>• edytor tekstów,<br>• arkusz kalkulacyjny,<br>• narzędzie do przygotowania i prowadzenia prezentacji,<br>• narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).<br>c. Edytor tekstów musi umożliwiać co najmniej:<br>• 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.<br>• Wstawianie oraz formatowanie tabel.<br>• Wstawianie oraz formatowanie obiektów graficznych.<br>• Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).<br>• Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.<br>• Automatyczne tworzenie spisów treści.<br>• Formatowanie nagłówków i stopek stron.<br>• Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.<br>• Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.<br>• Określenie układu strony (pionowa/pozioma).<br>• Wydruk dokumentów.<br>• Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.<br>• Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.<br>• Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.<br>d. Arkusz kalkulacyjny musi umożliwiać co najmniej:<br>• Tworzenie raportów tabelarycznych.<br>• Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych. |

| | |
|---|---|
| | • Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.<br>• Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice).<br>• Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych.<br>• Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.<br>• Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.<br>• Wyszukiwanie i zamianę danych.<br>• Wykonywanie analiz danych przy użyciu formatowania warunkowego.<br>• Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.<br>• Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.<br>• Formatowanie czasu, daty i wartości finansowych z polskim formatem.<br>• Zapis wielu arkuszy kalkulacyjnych w jednym pliku.<br>• Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.<br>e. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać co najmniej:<br>• Przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego.<br>• Drukowanie w formacie umożliwiającym robienie notatek.<br>• Zapisanie jako prezentacja tylko do odczytu.<br>• Nagrywanie narracji i dołączanie jej do prezentacji.<br>• Opatrywanie slajdów notatkami dla prezentera.<br>• Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.<br>• Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.<br>• Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.<br>• Możliwość tworzenia animacji obiektów i całych slajdów.<br>• Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.<br>f. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:<br>• Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.<br>• Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.<br>• Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.<br>• Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.<br>• Automatyczne grupowanie poczty o tym samym tytule.<br>• Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy. |

| | |
|---|---|
| | • Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.<br>• Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.<br>• Zarządzanie kalendarzem.<br>• Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.<br>• Przeglądanie kalendarza innych użytkowników.<br>• Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.<br>• Zarządzanie listą zadań.<br>• Zlecanie zadań innym użytkownikom.<br>• Zarządzanie listą kontaktów.<br>• Udostępnianie listy kontaktów innym użytkownikom.<br>• Przeglądanie listy kontaktów innych użytkowników.<br>Możliwość przesyłania kontaktów innym użytkowników. |
| **UPS (1 szt.)** | |
| Obudowa | RACK o rozmiarze maksymalnym 3U |
| Moc pozorna | minimum 3000 VA |
| Moc rzeczywista | minimum 2700 Wat. |
| Architektura UPS | line-interactive |
| Podtrzymanie | Liczba i rodzaj gniazdek z utrzymaniem zasilania: min. 6 szt. C13 |
| Podtrzymanie | Czas podtrzymania dla obciążenia 100%: min. 3 min. |
| Podtrzymanie | Czas podtrzymania przy obciążeniu 50%: min. 11 min. |
| Porty | 1 x USB, 1 x RJ45 |
| Funkcje | funkcja zimny start |
| Funkcje | awaryjne wyłączanie zasilania |

| | |
|---|---|
| Funkcje | ochrona przed nagłym wzrostem napięcia |
| Funkcje | baterie wymienne podczas pracy urządzenia |
| Funkcje | automatyczny test baterii |
| Obsługa | wyświetlacz LCD |
| Sygnalizacja | alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia |
| Gwarancja | gwarancja producenta min. 24 miesiące (w tym na baterię) |

## Część 2

| Lp. | Nazwa komponentu | Wymagane minimalne parametry |
|---|---|---|
| **UTM (1 szt.)** | | |
| 1. | Funkcjonalność | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. |
| 2. | Funkcjonalność | System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. |
| 3. | Funkcjonalność | System musi wspierać IPv4 oraz IPv6 w zakresie: firewall, ochrony w warstwie aplikacji, protokołów routingu dynamicznego. Wsparcie dla wszystkich głównych protokołów: HTTP, FTP, SMTP, POP3. |
| 4. | Redundancja, monitoring i wykrywanie awarii | 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. |
| 5. | Interfejsy | co najmniej 5 x Ethernet 10/100/1000. |
| 6. | Wydajność | Przepustowość firewall – co najmniej 10 Gbps, |
| 7. | Wydajność | Liczba równoległych sesji – co najmniej 700 000 jednoczesnych połaczeń |

| | | |
|---|---|---|
| 8. | Wydajność | Przepustowość IPsec VPN – co najmniej 6,5 Gbps |
| 9. | Wydajność | Liczba jednoczesnych klientów SSL VPN – co najmniej 200 |
| 10. | Wydajność | Wydajność SSL VPN: co najmniej 900 Mbps |
| 11. | Wydajność | Wsparcie VLAN: Musi posiadać minimum 50 sieci VLAN |
| 12. | Funkcje Systemu Bezpieczeństwa | • Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.<br>• Kontrola Aplikacji.<br>• Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.<br>• Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.<br>• Ochrona przed atakami - Intrusion Prevention System.<br>• Kontrola stron WWW.<br>• Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.<br>• Zarządzanie pasmem (QoS, Traffic shaping).<br>• Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.<br>• Analiza ruchu szyfrowanego protokołem SSL.<br>• Analiza ruchu szyfrowanego protokołem SSH. |
| 13. | Polityki firewall | • Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.<br>• 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. |
| 14. | Połączenia VPN | Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |
| 15. | Routing i obsługa łączy WAN | • Zapewnienie obsługi Routingu statycznego, Policy Based Routingu, protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM<br>• System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.<br>• Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.<br>• System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |

| | | |
|---|---|---|
| 16. | Kontrola antywirusowa | • Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.<br>• System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.<br>• System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).<br>• 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>• System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.<br>• Automatyczna aktualizacja plików sygnatur antywirusowych.<br>• Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji. |
| 17. | IPS | • Możliwość wsparcia IPS z poziomu urządzenia poprzez dodatkowe subskrypcje.<br>• Automatyczna aktualizacja sygnatur IPS.<br>• IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy. |
| 18. | Ochrona przed atakami | • System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.<br>• System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.<br>• Wykrywanie i blokowanie komunikacji C&C do sieci botnet.<br>• Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. |
| 19. | Zarządzanie | • Administracja urządzenia musi być możliwa poprzez graficzny interfejs zarządzania.<br>• Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.<br>• Rozwiązanie powinno umożliwiać wysyłanie alarmów przez SNMP lub e-mail.<br>• Urządzenie powinno mieć możliwość generowania raportów.<br>• 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>• Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.<br>• System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w |

| | | |
|---|---|---|
| | | wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. |
| 21. | Funkcje | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować następujące elementy: Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres gwarancji urządzenia. |
| 22. | Gwarancja | Gwarancja producenta: min. 24 miesiące |