1. Komputer stacjonarny. Typu All in One, komputer fabrycznie wbudowany w obudowę monitora. W ofercie wymagane jest podanie modelu producenta komputera - **2 szt.**

|  |  |
| --- | --- |
| Nazwa  | Wymagane minimalne parametry techniczne  |
| Typ | Komputer stacjonarny. Typu All in One, komputer fabrycznie wbudowany w obudowę monitora. W ofercie wymagane jest podanie modelu producenta komputera. |
| 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 | Komputer w oferowanej konfiguracji musi osiągać w teście wydajnościowym BAPCO wyniki nie gorsze niż:SYSmark 25 Overall Rating – co najmniej wynik 1500 punktówDokumentem potwierdzającym spełnianie ww. wymagań będzie dołączony do oferty wydruk raportu z oprogramowania testującego, potwierdzony za zgodność z oryginałem przez Wykonawcę.Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS ( tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testu Oferent może zostać wezwany do dostarczenia Zamawiającemu oprogramowania testującego, komputera do testów oraz dokładnego opisu metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego. |
| Pamięć RAM | 16GB DDR4 możliwość rozbudowy do 32GB RAM. |
| Pamięć masowa | 256GB SSDMożliwość instalacji dodatkowego dysku twardego M.2 lub 2.5 |
| Wydajność grafiki | Grafika zintegrowana z procesorem powinna umożliwiać pracę min. dwumonitorową, współdzielona i dynamicznie przydzielana pamięć z RAM, Karta osiągająca w teście PC Mark 10 Digital Content Creation wynik min. 4000 punktów – wynik załączyć do oferty. |
| Matryca | Rozmiar matrycy / plamki | min.23,8” / max. 0,275mm  |
| Rozdzielczość | FHD (1920x1080) |
| Jasność typowa | min. 250 cd/m²  |
| Kontrast typowy | 600:1 |
| Barwa koloru (typowa) | 72% NTSC |
| Kąty Horizontal/Vertical | 178(+/- 89) / 178 (+/-89) |
| Rodzaj matrycy | Matowa IPS |
| Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki min. 2W na kanał. Wbudowana w obudowę matrycy cyfrowa kamera 1.0 MP z diodą LED informującą użytkownika o pracy,Mechaniczna przesłona kamery w obudowie (nie dopuszcza się kamer przekręcanych).Wbudowane w obudowę dwa mikrofony  |
| Obudowa | Typu All-in-One zintegrowana z monitorem min. 23.8 cali. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki), Zasilacz o mocy min. 65W o efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, w szczególności: uszkodzenia lub braku pamięci RAM, uszkodzenia płyty głównej, awarii procesora. System diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji. Każdy komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz wpisanym na stałe w BIOS.Podstawa jednostki typu All – in – One musi umożliwiać:Regulację pochyłu pionowego w zakresie od -5 do 20 stopni. |
| Zgodność z systemami operacyjnymi i standardami | Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy). |
| Zdalne zarządzanie | Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową, a także zapewniająca min.:- Monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej; - Zdalną konfigurację ustawień BIOS |
| Bezpieczeństwo | Płyta główna zawierająca układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowegoZaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu boot’owania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego. |
| 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 myszy. (przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury).Informacje dostępne z poziomu BIOS na potrzeby inwentaryzacji:wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach, procesor (typ, nazwa, typowa prędkość, minimalna, maksymalna, cache L2 i L3) , pojemności zainstalowanego lub zainstalowanych dysków twardych MAC adres zintegrowanej karty sieciowej, zintegrowany układ graficzny, kontroler audio.Informacje dostępne w samym menu BIOS bez stosowania dodatkowego oprogramowania jak i wbudowanego systemu diagnostycznego.Możliwość, ustawienia hasła na poziomie:- administratora [hasło nadrzędne]- użytkownika/systemowego [hasło umożliwiające użytkownikowi zmianę swojego hasła i zgodnie z uprawnieniami nadanymi przez administratora dokonywać zmian ustawień BIOS], rozruch systemu operacyjnego [hasło blokuje start systemu operacyjnego].Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.Możliwość wyłączenia/włączenia karty sieciowejMożliwość włączenia/wyłączenia kontrolera SATAMożliwość włączenia/wyłączenia kontrolera audio,Możliwość włączenia/wyłączenia układu TPM.Możliwość włączenia/wyłączenia wbudowanej kamery i czytnika kart multimedialnychMożliwość włączenia/wyłączenia czujnika otwarcia obudowy, ustawienia go w tryb cichy Możliwość przypisania w BIOS numeru nadawanego przez Administratora oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym. [ musi umożliwiać znaki specjalne (@#$%^)]Możliwość zdefiniowania automatycznego uruchamiania komputera w min. dwóch trybach: codziennie lub w wybrane dni tygodnia,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.Możliwość wyłączania portów USB w szczególności pojedynczo w dowolnej kombinacja. BIOS musi nanosić automatycznie wszystkie zmiany konfiguracji dotyczące w szczególności: pamięci, procesora, dysku. |
| Certyfikaty i standardy | Certyfikat ISO9001 dla producenta sprzętu (załączyć do oferty)Certyfikat ISO 50001 dla producenta sprzętu (załączyć do oferty)Certyfikat ISO 45001 dla producenta sprzętu (załączyć do oferty)Deklaracja zgodności CE (załączyć do oferty)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 |
| System operacyjny – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | Zainstalowany system operacyjny Windows 11 Professional, klucz licencyjny musi umożliwiać instalację systemu operacyjnego zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego. |
| Wymagania dodatkowe  | Wbudowane porty: 1x HDMI 1x USB 3.2 Typ-C3x USB 3.2 Typ-A Wymagane porty USB wbudowane, nie dopuszcza się stosowania rozgałęziaczy, hub’ów itp. Wszystkie porty dostępne dla użytkownika w najniższej możliwej regulacji wysokości1x Universal audio jack 1x RJ-45 port 10/100/1000 MbpsKarta WiFi ax+ bluetooth 5.1Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w min. 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM, min. 1 złącza M.2 2280 dla dysku twardego oraz 1 złącze M.2 karty WiFi.Klawiatura USB w układzie polski programisty Mysz optyczna USB z dwoma przyciskami oraz rolką (scroll) |
| Dodatkowe oprogramowanie – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | Oprogramowanie producenta komputera z nieograniczoną czasowo licencją na użytkowanie umożliwiające:- upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi - dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne- włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji - sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania)- dostęp do wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml- dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu do pliku \*.xml Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku.W ofercie należy podać nazwę oprogramowania |
| Dodatkowe zabezpieczające – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | System chroniący przed zagrożeniami, posiadający certyfikaty: OPSWAT Platinum, AV-Test ‘Top Product’, AV Comperative Advance +, ISO 27001 . Silnik musi umożliwiać co najmniej:• wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,• wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,• stosowanie kwarantanny,• wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)• skanowanie urządzeń USB natychmiast po podłączeniu,• automatyczne odłączanie zainfekowanej końcówki od sieci,• skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji.• Zarządzanie „aktywami” stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach.• Musi posiadać moduł ochrony IDS/IPS• Musi posiadać mechanizm wykrywania skanowania portów• Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów• Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwościSzyfrowanie danych:• Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.• Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:• Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli• Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory• Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux• Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.• Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich• Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracjiZarządzanie przez Chmurę:1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznejCentralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer2. Oprogramowanie klienckie, zarządzane z poziomu serwera.System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:• różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie• funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD • funkcje regulowania połączeń WiFi i Bluetooth• funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe• funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi• funkcje blokowania dostępu dowolnemu urządzeniu• możliwość tymczasowego dodania dostępu do urządzenia przez administratora• zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu• możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka• możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora• możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry• możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich• funkcję wirtualnej klawiatury• możliwość blokowania każdej aplikacji • możliwość zablokowania aplikacji w oparciu o kategorie• możliwość dodania własnych aplikacji do listy zablokowanych• zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze• dodawanie innych aplikacji• dodawanie aplikacji w formie portable• możliwość wyboru pojedynczej aplikacji w konkretnej wersji • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB• kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool• możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.• możliwość zablokowania funkcji Printscreen• funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx• funkcje monitorowania i kontroli przepływu poufnych informacji• możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików• możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj• możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe• ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe• ochrona zawartości schowka systemu• ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL• możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych• ochrona plików zamkniętych w archiwach • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem• możliwość tworzenia profilu DLP dla każdej polityki• wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania • ochrona przez wyciekiem plików poprzez programy typu p2pMonitorowanie zmian w plikach:• Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.• Funkcje monitorowania określonych rodzajów plików.• Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.• Generator raportów do funkcjonalności monitora zmian w plikach.• możliwość śledzenia zmian we wszystkich plikach• możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach• możliwość definiowana własnych typów plikówOptymalizacja systemu operacyjnego stacji klienckich:• usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku• optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem• możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich• instruktaż stanowiskowy pracowników Zamawiającego• dokumentacja techniczna w języku polskimWspierane platformy i systemy operacyjne:1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)3. Mac OS X, Mac OS 104. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHatPlatforma do zarządzania dla Android i iOS:• Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę• Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.Zarządzanie użytkownikiem• Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email• Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika• Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi• Musi posiadać możliwość eksportu danych użytkownikaZarządzanie urządzeniem• Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO• Musi umożliwiać import listy urządzeń z pliku CSV• Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych• Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta• Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał• Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres• Musi zawierać podgląd aktualnie zainstalowanych aplikacji• Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, • Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł• Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakresOprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:Wymagania dotyczące technologii:1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:- Microsoft Internet Explorer- Microsoft Edge- Mozilla Firefox- Google Chrome- Safari4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:- Windows 2008 R2- Windows 2012- Windows 2012 R2- Windows 20167. Portal zarządzający musi umożliwiać:a) przegląd wybranych danych na podstawie konfigurowalnych widgetówb) zablokowania możliwości zmiany konfiguracji widgetówc) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatnoście) eksport wszystkich skanów podatności do pliku CSVBackup i przywracanie danych- Deduplikacja danych,- Backup przyrostowy i różnicowy,- Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,- Backup danych lokalnych – plikowy oraz poczty Outlook,- Backup otwartych plików (VSS),- Filtr plików oraz folderów,- Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.), - Wyłączanie komputera po wykonaniu backupu,- Przywracanie danych do wskazanej lokalizacji,- Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,- Wyszukiwanie plików w repozytorium użytkownika,Ustawienia- Automatyczne logowanie,- Zapamiętywanie danych logowania,- Automatyczne uruchamianie programu przy starcie systemu,- Ustawianie priorytetu dla procesu backupu,- Zmiana klucza szyfrującego,- Ustawienia przepustowości/zajętości pasma,- Konfiguracja wydajności procesu backupu,Bezpieczeństwo- Zastępowanie nazwy pliku GUID-em,- Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,- Kompresja danych,- Transmisja po bezpiecznym protokole TLS,- Deklaracja klucza szyfrującego dane użytkownika,- Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, - Obliczanie sumy kontrolnej,- Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski. WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze, Mac OS,Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji. |
| Warunki gwarancjiWsparcie techniczne | Minimum 2-letnia gwarancja producenta, Czas reakcji serwisu - do końca następnego dnia roboczego.W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta – wymagane dołączenie do oferty oświadczenia potwierdzonego, że serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez ProducentaDedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii. |

1. Monitor – 3 szt.

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne monitora** |
| Typ ekranu | Ekran ciekłokrystaliczny z aktywną matrycą LED, IPS lub VA 23,8”  |
| Jasność | 250 cd/m2 |
| Kontrast statyczny | 3000:1  |
| Kąty widzenia (pion/poziom) | 178/178 stopni |
| Czas reakcji matrycy | max 6 ms |
| Rozdzielczość maksymalna | 1920 x 1080 przy 60Hz |
| Wyświetlane kolory | 16.7 milionów |
| Zakres pochylenie monitora | +20°~-5°  |
| Powłoka powierzchni ekranu | Antyodblaskowa |
| Podświetlenie | System podświetlenia LED |
| Zużycie energii | Typowo 25W, czuwanie mniej niż 0,5W |
| Bezpieczeństwo | Monitor musi być wyposażony w tzw. Kensington Slot |
| Waga  | Maksymalnie 6 kg |
| Złącze  | DisplayPort - 1 szt.HDMI - 1 szt. |
| Gwarancja | 3 lata gwarancji z czasem reakcji serwisu - do końca następnego dnia roboczegoFirma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. |
| Inne | Odłączana stopa, VESA 100mmRedukcja migotania (Flicker free)Filtr światła niebieskiego głośniki 2x2W Regulacja wysokości monitora w zakresie min. 10cm.  |

1. **Microsoft Office Home & Business 2021 BOX lub równoważny Pakiet biurowy – 9 szt.**

# Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej.
2. Wymagania odnośnie interfejsu użytkownika:
	1. Pełna polska wersja językowa interfejsu użytkownika.
	2. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
3. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
	1. Posiada kompletny i publicznie dostępny opis formatu.
	2. Ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2

Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

* 1. Pozwala zapisywać dokumenty w formacie XML.
1. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb Zamawiającego.
2. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
3. Do aplikacji pakietu musi być dostępna pełna dokumentacja w języku polskim.
4. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
	1. Edytor tekstów.
	2. Arkusz kalkulacyjny.
	3. Narzędzie do przygotowywania i prowadzenia prezentacji.
	4. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).
5. Edytor tekstów musi umożliwiać:
	1. 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.
	2. Wstawianie oraz formatowanie tabel.
	3. Wstawianie oraz formatowanie obiektów graficznych.
	4. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
	5. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
	6. Automatyczne tworzenie spisów treści.
	7. Formatowanie nagłówków i stopek stron.
	8. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
	9. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
	10. Określenie układu strony (pionowa/pozioma), niezależnie dla każdej sekcji dokumentu.
	11. Wydruk dokumentów.
	12. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
	13. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007 lub Microsoft Word 2010, 2013, 2016 i 2019 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
	14. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
	15. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
	16. Wymagana jest dostępność mechanizmów umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
6. Arkusz kalkulacyjny musi umożliwiać:
	1. Tworzenie raportów tabelarycznych.
	2. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.
	3. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
	4. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML).
	5. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.
	6. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.
	7. Wyszukiwanie i zamianę danych.
	8. Wykonywanie analiz danych przy użyciu formatowania warunkowego.
	9. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.
	10. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
	11. Formatowanie czasu, daty i wartości finansowych z polskim formatem.
	12. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
	13. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 oraz Microsoft Excel 2010, 2013, 2016 i 2019, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
	14. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
7. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
	1. Przygotowywanie prezentacji multimedialnych, które będą:
	2. Prezentowanie przy użyciu projektora multimedialnego.
	3. Drukowanie w formacie umożliwiającym robienie notatek.
	4. Zapisanie jako prezentacja tylko do odczytu.
	5. Nagrywanie narracji i dołączanie jej do prezentacji.
	6. Opatrywanie slajdów notatkami dla prezentera.
	7. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.
	8. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.
	9. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.
	10. Możliwość tworzenia animacji obiektów i całych slajdów.
	11. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.
	12. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2007, MS PowerPoint 2010, 2013, 2016 i 2019.
8. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
	1. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.
	2. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.
	3. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.
	4. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.
	5. Automatyczne grupowanie wiadomości poczty o tym samym tytule.
	6. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.
	7. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.
	8. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.
	9. Zarządzanie kalendarzem.
	10. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.
	11. Przeglądanie kalendarza innych użytkowników.
	12. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.
	13. Zarządzanie listą zadań.
	14. Zlecanie zadań innym użytkownikom.
	15. Zarządzanie listą kontaktów.
	16. Udostępnianie listy kontaktów innym użytkownikom.
	17. Przeglądanie listy kontaktów innych użytkowników.
	18. Możliwość przesyłania kontaktów innym użytkowników.
	19. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.
9. 35 licencji dostępowych typu „na użytkownika” – Windows Server 2022 USER CALs

Opis równoważności:

1)     W celu utrzymania standaryzacji oprogramowania i pełnej jego kompatybilności, w opisie przedmiotu zamówienia wskazano znak towarowy firmy Microsoft ze względu na fakt rozszerzania posiadanych przez Zamawiającego licencji.

2)     W oparciu o art. 29 ust. 3 Ustawy z dnia 29.01.2004 r. Prawo zamówień publicznych wskazano znak towarowy firmy Microsoft jako wzorzec funkcjonalno-jakościowy przedmiotu Zamówienia.

3)   Oznacza to tym samym, że Zamawiający dopuszcza złożenie oferty na licencję dostępowego do oprogramowania serwerowego służącego do uzyskania dostępu do zasobów serwera będącego w posiadaniu Zamawiającego, o parametrach funkcjonalnych i jakościowych tożsamych z parametrami oprogramowania określonego we wzorcu, o ile jednocześnie zostaną zachowane pozostałe wymagania, określone w OPZ oraz zaoferowane licencje dostępowe do oprogramowania serwera będzie w pełni i poprawnie funkcjonowało z posiadanym i użytkowanym przez Zamawiającego oprogramowaniem serwera .

4)     Jednocześnie Zamawiający zakłada, że wykazanie równoważności złożonej oferty leży po stronie Wykonawcy i w razie wątpliwości powinno zostać udokumentowane w możliwie najbardziej obiektywny sposób.

5)     W przypadku zaoferowania przez Wykonawcę licencji dostępowych do oprogramowania serwerowego innego niż Microsoft Server, oświadczenie tego Wykonawcy zostanie przesłane do producenta ww. oprogramowania, celem jego weryfikacji.