*Załącznik nr 1*

Dotyczy zapytania ofertowego nr **01/06/2020/SSZ** w ramach projektu **„Szkoły sukcesu zawodowego”** współfinansowanego ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA:**

Przedmiotem zamówienia jest dostawa wraz z montażem wskazanego sprzętu technologii informacyjno-komunikacyjnej stanowiący wyposażenie szkolnych pracowni nauki zawodu :

**Poz. 1.** **wyposażenie do pracowni technik ekonomista - stanowisko komputerowe laptop dla nauczyciela– ilość szt.: 1**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
|  | Komputer | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. **W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.** |
|  | Ekran | Matryca TFT, 15,6” z podświetleniem w technologii LED, powłoka antyrefleksyjna Anti-Glare- rozdzielczość: FHD 1920x1080, 220nits |
|  | Obudowa | Obudowa komputera matowa, zawiasy metalowe. Kąt otwarcia matrycy min.130 stopni. W obudowie wbudowane co najmniej 2 diody sygnalizujące stan naładowania akumulatora oraz pracę dysku twardego. |
|  | Chipset | Dostosowany do zaoferowanego procesora |
|  | Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejs SATA III (6 Gb/s) do obsługi dysków twardych. Możliwość instalacji dwóch dysków twardych 1x M.2 oraz 1x 2.5. |
|  | Procesor | Procesor wielordzeniowy, osiągający w teście PassMark CPU Mark wynik min. 5000 punktów według wyników ze strony https://www.cpubenchmark.net/cpu\_list.php  **Wydruk załączyć do oferty.** |
| 1. . | Pamięć operacyjna | Min 8GB z możliwością rozbudowy do 32GB, rodzaj pamięci min. DDR4, 2400MHz. |
|  | Dysk twardy | Min. 256GB SSD M.2 zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |
|  | Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia do 2 GB pamięci.  Karta osiągająca w teście Average G3D Mark wynik min. 900 pkt. wynik dostępny na stronie: https://www.videocardbenchmark.net/ |
|  | Audio/Video | Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo min 2x 1,5W, wbudowany mikrofon, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute), kamera HD720p |
|  | Karta sieciowa | Zintegrowana z płytą główną 10/100/1000 – RJ 45 |
|  | Porty/złącza | 2xUSB 3.1, 1x USB 2.0, złącze słuchawek i złącze mikrofonu typu COMBO, 1xHDMI, RJ-45, czytnik kart multimedialnych (min SD/SDHC/SDXC). |
|  | Klawiatura | Klawiatura wyspowa, układ US. Klawiatura z wydzielonym blokiem numerycznym. |
|  | WiFi | Wbudowana karta sieciowa, pracująca w standardzie AC |
|  | Bluetooth | Wbudowany moduł Bluetooth 4.2 |
|  | Napęd optyczny | Wbudowana nagrywarka DVD o wysokości nie większej jak 9mm (możliwość wymiany napędu na drugą baterię) |
|  | Bateria | Bateria – 3 komorowa, 40 WHr pozwalająca na nieprzerwaną pracę urządzenia do 6 godzin. |
|  | Zasilacz | Zasilacz zewnętrzny max 65W |
|  | BIOS | BIOS zgodny ze specyfikacją UEFI. Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji: - wersji BIOS  - nr seryjnym komputera  - ilości pamięci RAM  - typie procesora i jego prędkości  -modele zainstalowanych dysków twardych  Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:   * Możliwość ustawienia hasła dla twardego dysku * Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password * Możliwość ustawienia hasła Administratora i użytkownika BIOS * Możliwość włączania/wyłączania wirtualizacji z poziomu BIOSU * Możliwość Wyłączania/Włączania: zintegrowanej karty WIFI, portów USB, Tryby PXE dla karty sieciowej,   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,  - 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 lub certyfikat równoważny dla producenta sprzętu (dostarczyć na wezwanie zamawiającego) * Deklaracja zgodności CE (dostarczyć na wezwanie zamawiającego) |
|  | System operacyjny – **w formularzu oferty trzeba podać nazwę oferowanego oprogramowania** | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:    1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,    2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. |
|  | Bezpieczeństwo i oprogramowanie dodatkowe – **w formularzu oferty trzeba podać nazwę oferowanego oprogramowania** | Licencja min. 2 lata: System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance + lub równoważny. 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 wrażliwości  Szyfrowanie danych:  • Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.  • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.  Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.  Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.  Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.  Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.  Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.  Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.  Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.  Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware  Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:  • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli  • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory  • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux  • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.  • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich  • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji  Zarządzanie przez Chmurę:  1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach  2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury  3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur  4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy  5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach  6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń  7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej  Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.  Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.  1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer  2. Oprogramowanie klienckie, zarządzane z poziomu serwera.  System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:  • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie  • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD  • funkcje regulowania połączeń WiFi i Bluetooth  • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe  • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi  • funkcje blokowania dostępu dowolnemu urządzeniu  • możliwość tymczasowego dodania dostępu do urządzenia przez administratora  • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu  • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka  • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora  • możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry  • możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich  • funkcję wirtualnej klawiatury  • możliwość blokowania każdej aplikacji  • możliwość zablokowania aplikacji w oparciu o kategorie  • możliwość dodania własnych aplikacji do listy zablokowanych  • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze  • dodawanie innych aplikacji  • dodawanie aplikacji w formie portable  • możliwość wyboru pojedynczej aplikacji w konkretnej wersji  • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB  • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool  • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.  • możliwość zablokowania funkcji Printscreen  • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx  • funkcje monitorowania i kontroli przepływu poufnych informacji  • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików  • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj  • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe  • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe  • ochrona zawartości schowka systemu  • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL  • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych  • ochrona plików zamkniętych w archiwach  • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem  • możliwość tworzenia profilu DLP dla każdej polityki  • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania  • ochrona przez wyciekiem plików poprzez programy typu p2p  Monitorowanie zmian w plikach:  • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.  • Funkcje monitorowania określonych rodzajów plików.  • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.  • Generator raportów do funkcjonalności monitora zmian w plikach.  • możliwość śledzenia zmian we wszystkich plikach  • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach  • możliwość definiowana własnych typów plików  Optymalizacja systemu operacyjnego stacji klienckich:  • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku  • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem  • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich  • instruktaż stanowiskowy pracowników Zamawiającego  • dokumentacja techniczna w języku polskim  Wspierane platformy i systemy operacyjne:  1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)  2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)  3. Mac OS X, Mac OS 10  4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat  Platforma do zarządzania dla Android i iOS:  • Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę  • Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.  Zarządzanie użytkownikiem  • Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email  • Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika  • Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi  • Musi posiadać możliwość eksportu danych użytkownika  Zarządzanie urządzeniem  • Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO  • Musi umożliwiać import listy urządzeń z pliku CSV  • Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych  • Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta  • Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał  • Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres  • Musi zawierać podgląd aktualnie zainstalowanych aplikacji  • Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych,  • Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł  • Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres  Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:  Wymagania dotyczące technologii:  1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową  2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.  3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:  - Microsoft Internet Explorer  - Microsoft Edge  - Mozilla Firefox  - Google Chrome  - Safari  4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących  5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie  6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:  - Windows 2008 R2  - Windows 2012  - Windows 2012 R2  - Windows 2016  7. Portal zarządzający musi umożliwiać:  a) przegląd wybranych danych na podstawie konfigurowalnych widgetów  b) zablokowania możliwości zmiany konfiguracji widgetów  c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.  d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności  e) eksport wszystkich skanów podatności do pliku CSV |
|  | Gwarancja | 3-letnia gwarancja, czas reakcji serwisu, do końca następnego dnia roboczego. Gwarancja musi oferować przez cały okres :  - mieć opiekę kierownika technicznego ds. Eskalacji  - dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu przez cały rok (w języku polskim w dni robocze)  Firma serwisująca musi posiadać ISO 9001:2000 lub równoważny certyfikat na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. |
|  | Wsparcie techniczne producenta | Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej.  - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego  - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |

**Poz. 2. wyposażenie do pracowni technik ekonomista - stanowisko komputerowe laptop dla ucznia – ilość szt.: 15**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
|  | Komputer | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej. **W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.** |
|  | Ekran | Matryca TFT, 15,6” z podświetleniem w technologii LED, powłoka antyrefleksyjna Anti-Glare- rozdzielczość: FHD 1920x1080, 220nits |
|  | Obudowa | Obudowa komputera matowa, zawiasy metalowe. Kąt otwarcia matrycy min.130 stopni. W obudowie wbudowane co najmniej 2 diody sygnalizujące stan naładowania akumulatora oraz pracę dysku twardego. |
|  | Chipset | Dostosowany do zaoferowanego procesora |
|  | Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejs SATA III (6 Gb/s) do obsługi dysków twardych. Możliwość instalacji dwóch dysków twardych 1x M.2 oraz 1x 2.5. |
|  | Procesor | Procesor wielordzeniowy, osiągający w teście PassMark CPU Mark wynik min. 5000 punktów według wyników ze strony https://www.cpubenchmark.net/cpu\_list.php  **Wydruk załączyć do oferty.** |
|  | Pamięć operacyjna | Min 8GB z możliwością rozbudowy do 32GB, rodzaj pamięci min. DDR4, 2400MHz. |
|  | Dysk twardy | Min. 256GB SSD M.2 zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |
|  | Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia do 2 GB pamięci.  Karta osiągająca w teście Average G3D Mark wynik min. 900 pkt. wynik dostępny na stronie: https://www.videocardbenchmark.net/ |
|  | Audio/Video | Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo min 2x 1,5W, wbudowany mikrofon, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute), kamera HD720p |
|  | Karta sieciowa | Zintegrowana z płytą główną 10/100/1000 – RJ 45 |
|  | Porty/złącza | 2xUSB 3.1, 1x USB 2.0, złącze słuchawek i złącze mikrofonu typu COMBO, 1xHDMI, RJ-45, czytnik kart multimedialnych (min SD/SDHC/SDXC). |
|  | Klawiatura | Klawiatura wyspowa, układ US. Klawiatura z wydzielonym blokiem numerycznym. |
|  | WiFi | Wbudowana karta sieciowa, pracująca w standardzie AC |
|  | Bluetooth | Wbudowany moduł Bluetooth 4.2 |
|  | Napęd optyczny | Wbudowana nagrywarka DVD o wysokości nie większej jak 9mm (możliwość wymiany napędu na drugą baterię) |
|  | Bateria | Bateria – 3 komorowa, 40 WHr pozwalająca na nieprzerwaną pracę urządzenia do 6 godzin. |
|  | Zasilacz | Zasilacz zewnętrzny max 65W |
|  | BIOS | BIOS zgodny ze specyfikacją UEFI. Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji: - wersji BIOS  - nr seryjnym komputera  - ilości pamięci RAM  - typie procesora i jego prędkości  -modele zainstalowanych dysków twardych  Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:   * Możliwość ustawienia hasła dla twardego dysku * Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password * Możliwość ustawienia hasła Administratora i użytkownika BIOS * Możliwość włączania/wyłączania wirtualizacji z poziomu BIOSU * Możliwość Wyłączania/Włączania: zintegrowanej karty WIFI, portów USB, Tryby PXE dla karty sieciowej,   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,  - 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 lub certyfikat równoważny dla producenta sprzętu (dostarczyć na wezwanie zamawiającego) * Deklaracja zgodności CE |
|  | System operacyjny – **w formularzu oferty trzeba podać nazwę oferowanego oprogramowania** | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:    1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,    2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. |
|  | Bezpieczeństwo i oprogramowanie dodatkowe licencja – **w formularzu oferty trzeba podać nazwę oferowanego oprogramowania** | Licencja min. 2 lata: System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance + lub równoważny. 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 wrażliwości  Szyfrowanie danych:  • Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.  • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.  Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.  Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.  Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.  Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.  Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.  Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.  Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.  Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware  Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:  • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli  • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory  • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux  • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.  • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich  • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji  Zarządzanie przez Chmurę:  1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach  2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury  3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur  4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy  5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach  6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń  7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej  Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.  Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.  1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer  2. Oprogramowanie klienckie, zarządzane z poziomu serwera.  System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:  • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie  • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD  • funkcje regulowania połączeń WiFi i Bluetooth  • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe  • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi  • funkcje blokowania dostępu dowolnemu urządzeniu  • możliwość tymczasowego dodania dostępu do urządzenia przez administratora  • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu  • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka  • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora  • możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry  • możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich  • funkcję wirtualnej klawiatury  • możliwość blokowania każdej aplikacji  • możliwość zablokowania aplikacji w oparciu o kategorie  • możliwość dodania własnych aplikacji do listy zablokowanych  • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze  • dodawanie innych aplikacji  • dodawanie aplikacji w formie portable  • możliwość wyboru pojedynczej aplikacji w konkretnej wersji  • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB  • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool  • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.  • możliwość zablokowania funkcji Printscreen  • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx  • funkcje monitorowania i kontroli przepływu poufnych informacji  • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików  • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj  • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe  • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe  • ochrona zawartości schowka systemu  • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL  • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych  • ochrona plików zamkniętych w archiwach  • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem  • możliwość tworzenia profilu DLP dla każdej polityki  • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania  • ochrona przez wyciekiem plików poprzez programy typu p2p  Monitorowanie zmian w plikach:  • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.  • Funkcje monitorowania określonych rodzajów plików.  • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.  • Generator raportów do funkcjonalności monitora zmian w plikach.  • możliwość śledzenia zmian we wszystkich plikach  • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach  • możliwość definiowana własnych typów plików  Optymalizacja systemu operacyjnego stacji klienckich:  • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku  • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem  • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich  • instruktaż stanowiskowy pracowników Zamawiającego  • dokumentacja techniczna w języku polskim  Wspierane platformy i systemy operacyjne:  1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)  2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)  3. Mac OS X, Mac OS 10  4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat  Platforma do zarządzania dla Android i iOS:  • Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę  • Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.  Zarządzanie użytkownikiem  • Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email  • Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika  • Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi  • Musi posiadać możliwość eksportu danych użytkownika  Zarządzanie urządzeniem  • Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO  • Musi umożliwiać import listy urządzeń z pliku CSV  • Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych  • Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta  • Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał  • Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres  • Musi zawierać podgląd aktualnie zainstalowanych aplikacji  • Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych,  • Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł  • Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres  Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:  Wymagania dotyczące technologii:  1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową  2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.  3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:  - Microsoft Internet Explorer  - Microsoft Edge  - Mozilla Firefox  - Google Chrome  - Safari  4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących  5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie  6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:  - Windows 2008 R2  - Windows 2012  - Windows 2012 R2  - Windows 2016  7. Portal zarządzający musi umożliwiać:  a) przegląd wybranych danych na podstawie konfigurowalnych widgetów  b) zablokowania możliwości zmiany konfiguracji widgetów  c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.  d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności  e) eksport wszystkich skanów podatności do pliku CSV |
|  | Gwarancja | 3-letnia gwarancja, czas reakcji serwisu, do końca następnego dnia roboczego. Gwarancja musi oferować przez cały okres :  - mieć opiekę kierownika technicznego ds. Eskalacji  - dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu przez cały rok (w języku polskim w dni robocze)  Firma serwisująca musi posiadać ISO 9001:2000 lub równoważny certyfikat na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. |
|  | Wsparcie techniczne producenta | Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej.  - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego  - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |

**Poz. 3.** **Specjalistyczne oprogramowanie do prowadzenia uproszczonych ewidencji podatkowych na 16 stanowisk– ilość szt.: 1**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
| 1 | Typ | Oprogramowanie do prowadzenia uproszczonych ewidencji podatkowych 1x16 stanowisk |
| 2 | Licencja | Okres obowiązywania min. 36 miesięcy |

**Poz. 4.** **program kadrowo-płacowy na 16 stanowisk– ilość szt.: 1**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
| 1 | Typ | Oprogramowanie kadrowo-płacowy na 16 stanowisk |
| 2 | Licencja | Okres obowiązywania min. 36 miesięcy |

**Poz. 5****. program do prowadzenia rozliczeń z Zakładem Ubezpieczeń Społecznych na 16 stanowisk– ilość szt.: 1**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
| 1 | Typ | Oprogramowanie do prowadzenia rozliczeń z Zakładem Ubezpieczeń Społecznych na 16 stanowisk |
| 2 | Licencja | Okres obowiązywania min. 36 miesięcy |

**Poz. 6****. program do wspomagania projektowania i wykonywania rysunków technicznych – ilość szt.: 1**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
|  |  | Program do projektowania kreślenia zawierający narzędzia do rysowania i detalowania 2D posiadający właściwości: Możliwość wymiarowania w tym inteligentnego wymiarowania i opisywania. Tworzenie i edytowanie dokładnych rysunków 2D. Program musi ułatwiać zadania dzięki intuicyjnemu interfejsowi oraz podręcznym narzędziom wbudowanym funkcjom. Umożliwia dostosowanie programu do indywidualnego sposobu pracy. Wbudowane zaawansowane narzędzia do tworzenia dokumentacji musza przekazywać rzeczywiste wymiary i szczegóły techniczne, które odzwierciedlają specyfikę danego projektu. Program musi mieć wbudowane standardowe kształty takie jak linie, wielokąty, luki, okręgi i elipsy, aby tworzyć proste lub złożone rysunki 2D. Program umożliwia modyfikowanie obiektów. Program zmienia istniejące geometrie za pomocą takich poleceń jak rozciągnij, skala i obróć. Musi mieć wbudowane polecenia tworzenia nowych obiektów, kopiowania, odsunięcia i lustra. Program musi umożliwiać opisywanie rysunków oraz ich uzupełnianie np. opisami tekstowymi, wymiarowaniami, kreskowaniami i współpracę z rodziną programów Autdesk.. Program Musi umożliwiać pracę z plikami w formacie \*.DWG. Musi posiadać obsługę dynamicznych bloków, ukrywanie i izolowanie wybranych obiektów, obsługa przeźroczystości warstw, możliwość łączenia rysunków z plikami zewnętrznymi (np. jpg, pdf), czy automatyczne autouzupełnianie poleceń. Program musi umożliwiać publikowanie i drukowanie. Program musi umożliwiać tworzenie wieloarkuszowych plików DWF, DWFx i PDF. |

**Poz. 7.** **Drukarka 3D – ilość szt.: 1**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
|  | Technologia druku | Min. FFF lub FDM |
|  | Pole robocze | Min. 199 x 199 x 199 mm |
|  | Kompatybilne filamenty | Min. ABS, PLA, PETG lub PVA lub CPE |
|  | Średnica dyszy/wytłaczarki | Min. 0,4 mm |
|  | Temperatura dyszy | Min. 230 stopni |
|  | Obsługiwane typy plików | Min. STL, OBJ, 3MF lub DAE |
|  | Gwarancja | Min. 12 miesięcy |

**Poz. 8.** **Dysk zewnętrzny 1TB – ilość szt.: 1**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
|  | Rodzaj Dysku | HDD lub SSD |
|  | Pojemność | Min. 2TB |
|  | Złącza | Min. USB 3.0 |
|  | Gwarancja | Min. 36 miesięcy |

**Poz. 9.** **Zestawy multimedialne (Tablica interaktywna, półka interaktywna, głośniki, Laptop) – ilość szt.: 7  
I.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
|  | Tablica interaktywna | Technologia pozycjonowania w podczerwieni, dotykowa,  Precyzja dotyku przynajmniej < 1mm  Obsługa dotyku: palec, pisak, wskaźnik, dowolny nieprzezroczysty obiekt |
|  | Format obrazu, rozdzielczość | Format min. 4:3, Rozdzielczość min. 32700 x 32700 |
|  | Powierzchnia | Ceramiczna, matowa, magnetyczna o wysokiej odporności na zarysowania, łatwa do czyszczenia, dostosowana do używania pisaków suchościeralnych, |
|  | Walory użytkowe | Sterowanie min. 10 aktywnymi punktami na obszarze interaktywnym tablicy; Plug and play, tablica po podłączeniu do komputera jest aktywna nie ma konieczności instalowania sterowników |
|  | Oprogramowanie interaktywne  producenta tablicy | Bogate, funkcjonalne i intuicyjne oprogramowanie pozwala na realizację funkcji, jak : rozpoznawanie pisma odręcznego, zrzuty odtwarzanie video z możliwością „pisania” na filmie szybkie tworzenie figur geometrycznych.  Program posiada bogatą bibliotekę załączników związanych z przedmiotami szkolnymi , min modele 3D figur geometrycznych czy zwierząt . Integruje się z programami pakietu MS Office pozwalając na ręczne dopisywanie notatek do dokumentów.  Zdalna komunikacja z poziomu smartfonów czy tabletów z Tablicą wykonywanie zadań dla nauczyciela/ucznia. |
|  | Usługi | Wsparcie serwisu technicznego, telefonicznie lub online.  Montaż oraz w dniu montażu: szkolenie techniczne , wdrożenie do eksploatacji z instruktażem z obsługi i funkcjonalności urządzeń. |
|  | Certyfikaty | CE |
|  | Gwarancja | Min. 3 lat na na tablicę, min. 25 lat na powierzchnię, min. 1 rok na pozostałe elementy. |
|  | Wyposażenie | Głośniki: kompatybilne z tablicą interaktywną, montowane na bokach tablicy, nie dopuszcza się montażu głośników na ścianie.  Moc min. 2x20 W. Minimalne wyposażenie: Półka na pisaki, pisaki min. 4 sztuki kabel USB, uchwyty do montażu na ścianie, wskaźnik.  Półka interaktywna: aktywowanie wybranego koloru pisaka po przez podniesienie go z półki. |

**II.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
|  | Projektor | Min. Krótkoogniskowy |
|  | Technologia | LCD |
|  | Jasność | Min. 3000 ANSI |
|  | Rozdzielczość | Min. XGA 1024x768, format 4:3 (kompatybilny z tablicą interaktywną) |
|  | Kontrast | Min. 6000:1 |
|  | Lampa | Moc min. 210W. żywotność min. 8000h |
|  | Rozmiar  projekcji (przekątna) | Możliwość rzutu ekranu o regulacji przekątnej min. w zakresie  62-100” |
|  | Złącza wbudowane | Min. 2x VGA, 1xVGA lub 1xHDMI, 1xHDMI, 2x USB, 1x komponent |
|  | Głośniki wbudowane | Min. 16W |
|  | Wyposażenie | Uchwyt ścienny w zestawie, okablowanie zasilające, HDMI min. 10m |
|  | Gwarancja | Min. 60 miesięcy, Lampa 60 miesięcy lub 1000h |

**III.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
|  | Komputer | Komputer będzie wykorzystywany w zestawie z tablicą interaktywną. **W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.** |
|  | Ekran | Matryca TFT, 15,6” z podświetleniem w technologii LED, powłoka antyrefleksyjna Anti-Glare- rozdzielczość: FHD 1920x1080, 220nits |
|  | Obudowa | Obudowa komputera matowa, zawiasy metalowe. Kąt otwarcia matrycy min.130 stopni. W obudowie wbudowane co najmniej 2 diody sygnalizujące stan naładowania akumulatora oraz pracę dysku twardego. |
|  | Chipset | Dostosowany do zaoferowanego procesora |
|  | Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejs SATA III (6 Gb/s) do obsługi dysków twardych. Możliwość instalacji dwóch dysków twardych 1x M.2 oraz 1x 2.5. |
|  | Procesor | Procesor wielordzeniowy, osiągający w teście PassMark CPU Mark wynik min. 5000 punktów według wyników ze strony https://www.cpubenchmark.net/cpu\_list.php  **Wydruk ze strony załączyć do oferty** |
| 1. . | Pamięć operacyjna | Min 8GB z możliwością rozbudowy do 32GB, rodzaj pamięci min. DDR4, 2400MHz. |
|  | Dysk twardy | Min. 256GB SSD M.2 zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |
|  | Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia do 2 GB pamięci.  Karta osiągająca w teście Average G3D Mark wynik min. 900 pkt. wynik dostępny na stronie: https://www.videocardbenchmark.net/ |
|  | Audio/Video | Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo min 2x 1,5W, wbudowany mikrofon, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute), kamera HD720p |
|  | Karta sieciowa | Zintegrowana z płytą główną 10/100/1000 – RJ 45 |
|  | Porty/złącza | 2xUSB 3.1, 1x USB 2.0, złącze słuchawek i złącze mikrofonu typu COMBO, 1xHDMI, RJ-45, czytnik kart multimedialnych (min SD/SDHC/SDXC). |
|  | Klawiatura | Klawiatura wyspowa, układ US. Klawiatura z wydzielonym blokiem numerycznym. |
|  | WiFi | Wbudowana karta sieciowa, pracująca w standardzie AC |
|  | Bluetooth | Wbudowany moduł Bluetooth 4.2 |
|  | Napęd optyczny | Wbudowana nagrywarka DVD o wysokości nie większej jak 9mm (możliwość wymiany napędu na drugą baterię) |
|  | Bateria | Bateria – 3 komorowa, 40 WHr pozwalająca na nieprzerwaną pracę urządzenia do 6 godzin. |
|  | Zasilacz | Zasilacz zewnętrzny max 65W |
|  | BIOS | BIOS zgodny ze specyfikacją UEFI. Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji: - wersji BIOS  - nr seryjnym komputera  - ilości pamięci RAM  - typie procesora i jego prędkości  -modele zainstalowanych dysków twardych  Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:   * Możliwość ustawienia hasła dla twardego dysku * Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password * Możliwość ustawienia hasła Administratora i użytkownika BIOS * Możliwość włączania/wyłączania wirtualizacji z poziomu BIOSU * Możliwość Wyłączania/Włączania: zintegrowanej karty WIFI, portów USB, Tryby PXE dla karty sieciowej,   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,  - 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 lub równoważny dla producenta sprzętu (Dostarczyć na wezwanie zamawiającego) * Deklaracja zgodności CE |
|  | System operacyjny – **w formularzu oferty trzeba podać nazwę oferowanego oprogramowania** | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:   1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:    1. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,    2. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. |
|  | Bezpieczeństwo i oprogramowanie dodatkowe – **w formularzu oferty trzeba podać nazwę oferowanego oprogramowania** | Licencja min. 2 lata: System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance + lub równoważny. 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 wrażliwości  Szyfrowanie danych:  • Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.  • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.  Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.  Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.  Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.  Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.  Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.  Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.  Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.  Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware  Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:  • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli  • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory  • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux  • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.  • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich  • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji  Zarządzanie przez Chmurę:  1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach  2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury  3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur  4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy  5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach  6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń  7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej  Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.  Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.  1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer  2. Oprogramowanie klienckie, zarządzane z poziomu serwera.  System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:  • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie  • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD  • funkcje regulowania połączeń WiFi i Bluetooth  • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe  • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi  • funkcje blokowania dostępu dowolnemu urządzeniu  • możliwość tymczasowego dodania dostępu do urządzenia przez administratora  • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu  • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka  • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora  • możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry  • możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich  • funkcję wirtualnej klawiatury  • możliwość blokowania każdej aplikacji  • możliwość zablokowania aplikacji w oparciu o kategorie  • możliwość dodania własnych aplikacji do listy zablokowanych  • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze  • dodawanie innych aplikacji  • dodawanie aplikacji w formie portable  • możliwość wyboru pojedynczej aplikacji w konkretnej wersji  • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB  • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool  • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.  • możliwość zablokowania funkcji Printscreen  • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx  • funkcje monitorowania i kontroli przepływu poufnych informacji  • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików  • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj  • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe  • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe  • ochrona zawartości schowka systemu  • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL  • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych  • ochrona plików zamkniętych w archiwach  • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem  • możliwość tworzenia profilu DLP dla każdej polityki  • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania  • ochrona przez wyciekiem plików poprzez programy typu p2p  Monitorowanie zmian w plikach:  • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.  • Funkcje monitorowania określonych rodzajów plików.  • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.  • Generator raportów do funkcjonalności monitora zmian w plikach.  • możliwość śledzenia zmian we wszystkich plikach  • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach  • możliwość definiowana własnych typów plików  Optymalizacja systemu operacyjnego stacji klienckich:  • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku  • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem  • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich  • instruktaż stanowiskowy pracowników Zamawiającego  • dokumentacja techniczna w języku polskim  Wspierane platformy i systemy operacyjne:  1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)  2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)  3. Mac OS X, Mac OS 10  4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat  Platforma do zarządzania dla Android i iOS:  • Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę  • Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.  Zarządzanie użytkownikiem  • Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email  • Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika  • Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi  • Musi posiadać możliwość eksportu danych użytkownika  Zarządzanie urządzeniem  • Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO  • Musi umożliwiać import listy urządzeń z pliku CSV  • Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych  • Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta  • Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał  • Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres  • Musi zawierać podgląd aktualnie zainstalowanych aplikacji  • Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych,  • Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł  • Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres  Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:  Wymagania dotyczące technologii:  1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową  2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.  3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:  - Microsoft Internet Explorer  - Microsoft Edge  - Mozilla Firefox  - Google Chrome  - Safari  4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących  5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie  6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:  - Windows 2008 R2  - Windows 2012  - Windows 2012 R2  - Windows 2016  7. Portal zarządzający musi umożliwiać:  a) przegląd wybranych danych na podstawie konfigurowalnych widgetów  b) zablokowania możliwości zmiany konfiguracji widgetów  c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.  d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności  e) eksport wszystkich skanów podatności do pliku CSV |
|  | Gwarancja | 3-letnia gwarancja, czas reakcji serwisu, do końca następnego dnia roboczego. Gwarancja musi musi oferować przez cały okres :  - mieć opiekę kierownika technicznego ds. Eskalacji  - dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu przez cały rok (w języku polskim w dni robocze)  Firma serwisująca musi posiadać ISO 9001:2000 lub certyfikat równoważny na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. |
|  | Wsparcie techniczne producenta | Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej.  - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego  - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |

**Poz. 10.** **Oprogramowanie dla grafików na 25 stanowisk – ilość szt.: 1**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
|  | Funkcjonalność | Program służący do edytowania i obróbki zdjęć oraz grafiki rastrowej. |
|  | Wymagania minimalne | Program posiada możliwość:  Obrabiania obrazów HDR  Płynnego obracania obszaru roboczego  Wprowadzania efektów malowania  Automatycznej korekty obrazu  Automatycznego zapisu w tle  Automatycznego odzyskiwania  Redukowania potrząśnięć aparatem fotograficznym  Rozszerzania i przesuwania z uwzględnieniem zawartości  Skalowania i obracania  Wypaczania perspektywy  Tworzenia obiektów 3D oraz ich animowanie  Program musi posiadać możliwość stosowania konwersji na obrazy monochromatyczne, wielu instancji styków warstw oraz posiada w swojej funkcjonalności narzędzia wyostrzania, próbkowania i korekty. Obsługuje natywnie formaty plików TIFF, AI, PDF, SVG, DWG, DXF. |
|  | Licencja | Licencja na okres nie krótszy niż 24 miesiące. |

**Poz. 11.** **Oprogramowanie Impozycjoner na 16 stanowisk (zmienić) – ilość szt.: 1**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
|  | Funkcjonalność | Program służący do wspomagania impozycji plików w formacie pdf. Można za jego pomocą montować akcydensy oraz arkusze falcowane i niefalcowane |
|  | Licencja | Licencja na okres nie krótszy niż 60 miesięcy |

**Poz. 12.** **Oprogramowanie do projektowania grafiki na 16 stanowisk– ilość szt.: 1**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
|  | Funkcjonalność | Program służący do projektowania grafiki, obróbki grafiki wektorowej i rastrowej |
|  | Wymagania minimalne | Program posiada następującą funkcjonalność:  Interfejs użytkownika podlegający pełnej konfiguracji  Obszar projektowania podlegający pełnej konfiguracji użytkownika  Możliwość pracy na wielu dokumentach przy użyciu widoku kart  Możliwość oddokowania okna pracy  Możliwość pełnego wykorzystania tabletów graficznych wraz z piórkami czułymi na nacisk i nachylenie  Obsługa funkcji dotyku  Wycinanie i kopiowanie segmentów krzywych  Redukcja postrzępionych krawędzi  Ograniczanie liczby węzłów  Określanie położenia i rozmiaru obiektów w precyzyjny sposób  Przeglądanie, filtrowanie i przeszukiwanie czcionek za pomocą wbudowanego narzędzia  Korekcja zniekształcenia perspektywy  Zwiększanie ostrości na zdjęciach  Tworzenie alfanumerycznych, dwuwymiarowych, matrycowych, kwadratowych kodów kreskowych  Nakładanie maski na obiekty bez ich modyfikacji  Przekształcanie grafiki rastrowej na wektorową |
|  | Licencja | Licencja na okres nie krótszy niż 36 miesięcy |

**Poz. 13.** **Komputery do obróbki grafiki i multimediów Pracownia 1– ilość szt.: 16**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** | |
|  | Typ | | Komputer stacjonarny. |
|  | Zastosowanie | | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej |
|  | Procesor | | Procesor czterordzeniowy, taktowany częstotliwością bazowa co najmniej 3.6 GHz. Wydajność procesora spełniająca kryterium PassMark >= 7870 wg klasyfikacji CPU Benchmark dostępnej pod adresem: <https://www.cpubenchmark.net> **Wydruk ze strony załączyć do oferty** |
|  | Pamięć operacyjna | | Min. 1x8GB DDR4 2400MHz, możliwość rozbudowy do min 32GB. Obsługa pamięci DDR4 1866/ 2133/ 2400/ 2667(OC)/ 2933(OC)/3200(OC)+ MHz |
|  | Parametry pamięci masowej | | Min. 256GB SSD  Płyta ze wsparciem dla dysków M.2 NVMe 22110. |
|  | Grafika | | Karta graficzna z min. 2GB pamięci własnej, złącza video: min. 1xHDMI. Karta osiągająca w teście Average G3D Mark wynik min. 2270pkt., wynik dostępny na stronie: <https://www.videocardbenchmark.net/> |
|  | Wyposażenie multimedialne | | Karta dźwiękowa zintegrowana z płytą główną, min. 2 kanałowa; |
|  | Obudowa | | Obudowa mini lub mikro tower o wymiarach nie większych niż 35x15x30 cm, możliwość montażu pełnowymiarowych kart graficznych, montaż beznarzędziowy dysków; napędu optycznego i kart rozszerzeń; wykonana z blachy o grubości co najmniej 0,6mm  możliwość montażu dysku 2x2,5" oraz 1x 3,5" wewnątrz obudowy  wyposażona w 2 porty USB 3.1 oraz złącza mikrofonu i słuchawek z przodu obudowy  wbudowana karta sieciowa 10/100/100  możliwość otwierania bez użycia narzędzi (wkręty ręczne)  wyposażona w złącze Kensington Lock i ucho na kłódkę  Zasilacz o mocy minimum 300W 80+ Bronze. Zasilacz w oferowanym komputerze musi znajdować się na stronie internetowej <http://www.plugloadsolutions.com/80pluspowersupplies.aspx> (**Wydruk załączyć na wezwanie zamawiającego**). |
|  | Certyfikaty i standardy | | * Deklaracja zgodności CE * Produkcja sprzętu zgodnie z ISO 9001, ISO 27001, ISO 28000 lub równoważne |
|  | BIOS | | * BIOS zgodny ze specyfikacją UEFI * Możliwość obsługi klawiaturą oraz myszą * Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji: * wersji BIOS, * nr seryjnym komputera, * ilości pamięci RAM, * typie procesora, * pojemności zainstalowanego dysku twardego * rodzajach napędów optycznych * kontrolerze audio * Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego * Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń * BIOS ma być w pełni obsługiwany przez interfejs myszy i klawiatury oraz w pełni wykorzystywać dyski twarde większe niż 2.2TB |
|  | System operacyjny – w formularzu oferty należy podać wersje oferowanego oprogramowania | | Parycja Recovery umożliwiająca w przypadku awarii dysku twardego ponowną instalację zainstalowanego systemu operacyjnego oraz nośnik zawierający sterowniki wszystkich zainstalowanych urządzeń.  System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego  3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim  4. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe  5. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,  6. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.  7. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim  8. Wbudowany system pomocy w języku polskim.  9. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).  10. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące  11. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń  12. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń  13. Możliwość pracy w domenie Active Directory |
|  | Bezpieczeństwo i oprogramowanie dodatkowe – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | | Licencjamin.2lata: System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. 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 wrażliwości  Szyfrowanie danych:  • Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.  • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.  Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.  Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.  Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.  Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.  Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.  Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.  Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.  Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware  Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:  • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli  • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory  • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux  • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.  • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich  • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji  Zarządzanie przez Chmurę:  1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach  2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury  3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur  4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy  5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach  6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń  7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej  Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.  Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.  1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer  2. Oprogramowanie klienckie, zarządzane z poziomu serwera.  System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:  • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie  • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD  • funkcje regulowania połączeń WiFi i Bluetooth  • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe  • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi  • funkcje blokowania dostępu dowolnemu urządzeniu  • możliwość tymczasowego dodania dostępu do urządzenia przez administratora  • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu  • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka  • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora  • możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry  • możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich  • funkcję wirtualnej klawiatury  • możliwość blokowania każdej aplikacji  • możliwość zablokowania aplikacji w oparciu o kategorie  • możliwość dodania własnych aplikacji do listy zablokowanych  • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze  • dodawanie innych aplikacji  • dodawanie aplikacji w formie portable  • możliwość wyboru pojedynczej aplikacji w konkretnej wersji  • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB  • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool  • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.  • możliwość zablokowania funkcji Printscreen  • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx  • funkcje monitorowania i kontroli przepływu poufnych informacji  • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików  • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj  • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe  • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe  • ochrona zawartości schowka systemu  • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL  • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych  • ochrona plików zamkniętych w archiwach  • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem  • możliwość tworzenia profilu DLP dla każdej polityki  • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania  • ochrona przez wyciekiem plików poprzez programy typu p2p  Monitorowanie zmian w plikach:  • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.  • Funkcje monitorowania określonych rodzajów plików.  • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.  • Generator raportów do funkcjonalności monitora zmian w plikach.  • możliwość śledzenia zmian we wszystkich plikach  • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach  • możliwość definiowana własnych typów plików  Optymalizacja systemu operacyjnego stacji klienckich:  • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku  • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem  • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich  • instruktaż stanowiskowy pracowników Zamawiającego  • dokumentacja techniczna w języku polskim  Wspierane platformy i systemy operacyjne:  1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)  2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)  3. Mac OS X, Mac OS 10  4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat  Platforma do zarządzania dla Android i iOS:   * Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę * Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.   Zarządzanie użytkownikiem   * Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email * Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika * Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi * Musi posiadać możliwość eksportu danych użytkownika   Zarządzanie urządzeniem   * Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO * Musi umożliwiać import listy urządzeń z pliku CSV * Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych * Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta * Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał * Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres * Musi zawierać podgląd aktualnie zainstalowanych aplikacji * Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, * Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł * Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres   Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:  Wymagania dotyczące technologii:   1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową 2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta. 3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:   - Microsoft Internet Explorer  - Microsoft Edge  - Mozilla Firefox  - Google Chrome  - Safari   1. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących 2. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 3. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:   - Windows 2008 R2  - Windows 2012  - Windows 2012 R2  - Windows 2016  7. Portal zarządzający musi umożliwiać:  a)           przegląd wybranych danych na podstawie konfigurowalnych widgetów  b)           zablokowania możliwości zmiany konfiguracji widgetów  c)            zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.  d)           tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności  e)           eksport wszystkich skanów podatności do pliku CSV |
| 13. | Gwarancja i wsparcie techniczne producenta | 3-letnia gwarancja producenta, Czas reakcji serwisu do końca następnego dnia roboczego. Firma serwisująca musi posiadać ISO 9001:2000 lub certyfikat równoważny na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające dostarczyć na wezwanie zamawiającego  Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera, dostępna w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia:  - weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa - CPU, HDD, pamięć)  Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera | |
| 14 | Wymagania dodatkowe | Wbudowane porty:  • min. 1 x VGA,  • min. 1 x DVI  • min. 1 x HDMI ver. 1.4  • min. 2 x PS/2,  • min. 8 portów USB wyprowadzonych na zewnątrz komputera w tym min.: min. 2 porty USB 3.1 z przodu obudowy, 4szt. USB 3.1 z tyłu obudowy - wymagana ilość i rozmieszczenie portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, kart PCIe itp.  • porty słuchawek i mikrofonu na przednim oraz tylnym panelu obudowy.  • Komputer musi umożliwiać jego rozbudowę w postaci dedykowanych kart PCIe np. kartę WiFi a/b/g/n  • Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), PXE 2.1.  • Płyta główna posiadająca chipset rekomendowany przez producenta procesora. Zbudowana w oparciu o kondensatory polimerowe o podwyższonej trwałości., przeznaczona dla danego urządzenia; wyposażona w :   * SATA III (6 Gb/s) - 4 szt. * M.2 - 1 szt. * PCIe 3.0 x16 - 1 szt. * PCIe 2.0 x1 - 2 szt. * Złącze wyjścia S/PDIF - 1 szt. * 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM, z obsługą DDR4-3200 MHz   • Klawiatura USB w układzie polski programisty  • Mysz USB z klawiszami oraz rolką (scroll)  • Wbudowana w obudowę nagrywarka DVD +/-RW szybkość min. x24 wraz z oprogramowaniem do nagrywania i odtwarzania płyt  • Dołączony nośnik ze sterownikami   * Wsparcie dla konfiguracji RAID 0, 1, 10   Wbudowany w płytę główną układ przetwarzania energii, zapewniający możliwość całościowego zarządzania poziomem zużywanej energii poprzez wykrywanie aktualnego poziomu wykorzystania zasobów PC (CPU, GPU, HDD, zasilacza) oraz inteligentne przydzielanie mocy w czasie rzeczywistym. Układ działający automatycznie od momentu uruchomienia komputera.  Ochrona przed nadmiernym napięciem zasilania:  System zasilania chroniący obwód specjalnie zaprojektowany przez producenta płyty głównej z wbudowanymi regulatorami napięcia do ochrony chipsetu, gniazd połączeniowych i kodeków audio przed uszkodzeniem spowodowanym nieoczekiwanymi napięciami wysokiej wartości z niestabilnych albo złych zasilaczy. | |
|  | Monitor, Typ ekranu | Ekran ciekłokrystaliczny LED, IPS 21,5” | |
|  | Jasność | 250 cd/m2 | |
|  | Kontrast | 10 000 000:1 | |
|  | Kąty widzenia (pion/poziom) | 178/178 stopni | |
|  | Czas reakcji matrycy | max 1 ms | |
|  | Rozdzielczość maksymalna | 1920 x 1080 przy 60Hz | |
|  | Wyświetlane kolory | 16.7 milionów | |
|  | Pochylenie | Tak | |
|  | Powłoka powierzchni ekranu | Antyodblaskowa | |
|  | Podświetlenie | System podświetlenia LED | |
|  | Zużycie energii | Typowo 15W, czuwanie mniej niż 0,5W | |
|  | Bezpieczeństwo | Monitor musi być wyposażony w tzw. Kensington Slot | |
|  | Złącze | VGA (D-sub) - 1 szt.  HDMI - 1 szt.  Wyjście słuchawkowe - 1 szt.  Wejście audio - 1 szt. | |
|  | Gwarancja | 3 lata gwarancji z czasem reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001:2000 lub certyfikat równoważny na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. | |
|  | Certyfikaty | CE | |
|  | Inne | Wbudowane w obudowę głośniki stereo o mocy min. 2W.  Odłączana stopa, VESA 100mm | |

**Poz. 14.** **Komputery do obróbki grafiki i multimediów Pracownia 2– ilość szt.: 7**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
|  | Typ | Komputer stacjonarny. |
|  | Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej |
|  | Procesor | Procesor czterordzeniowy, taktowany częstotliwością bazowa co najmniej 3.6 GHz. Wydajność procesora spełniająca kryterium PassMark >= 7870 wg klasyfikacji CPU Benchmark dostępnej pod adresem: <https://www.cpubenchmark.net> |
|  | Pamięć operacyjna | Min. 1x8GB DDR4 2400MHz, możliwość rozbudowy do min 32GB. Obsługa pamięci DDR4 1866/ 2133/ 2400/ 2667(OC)/ 2933(OC)/3200(OC)+ MHz |
|  | Parametry pamięci masowej | Min. 256GB SSD  Płyta ze wsparciem dla dysków M.2 NVMe 22110. |
|  | Grafika | Karta graficzna z min. 2GB pamięci własnej, złącza video: min. 1xHDMI. Karta osiągająca w teście Average G3D Mark wynik min. 2270pkt., wynik dostępny na stronie: <https://www.videocardbenchmark.net/> |
|  | Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, min. 2 kanałowa; |
|  | Obudowa | Obudowa mini lub mikro tower o wymiarach nie większych niż 35x15x30 cm, możliwość montażu pełnowymiarowych kart graficznych, montaż beznarzędziowy dysków; napędu optycznego i kart rozszerzeń; wykonana z blachy o grubości co najmniej 0,6mm  możliwość montażu dysku 2x2,5" oraz 1x 3,5" wewnątrz obudowy  wyposażona w 2 porty USB 3.1 oraz złącza mikrofonu i słuchawek z przodu obudowy  wbudowana karta sieciowa 10/100/100  możliwość otwierania bez użycia narzędzi (wkręty ręczne)  wyposażona w złącze Kensington Lock i ucho na kłódkę  Zasilacz o mocy minimum 300W 80+ |
|  | Certyfikaty i standardy | * Deklaracja zgodności CE * Produkcja sprzętu zgodnie z ISO 9001, ISO 27001, ISO 28000 lub równoważne |
|  | BIOS | * BIOS zgodny ze specyfikacją UEFI * Możliwość obsługi klawiaturą oraz myszą * Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji: * wersji BIOS, * nr seryjnym komputera, * ilości pamięci RAM, * typie procesora, * pojemności zainstalowanego dysku twardego * rodzajach napędów optycznych * kontrolerze audio * Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego * Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń * BIOS ma być w pełni obsługiwany przez interfejs myszy i klawiatury oraz w pełni wykorzystywać dyski twarde większe niż 2.2TB |
|  | System operacyjny – w formularzu oferty należy podać wersje oferowanego oprogramowania | Parycja Recovery umożliwiająca w przypadku awarii dysku twardego ponowną instalację zainstalowanego systemu operacyjnego oraz nośnik zawierający sterowniki wszystkich zainstalowanych urządzeń.  System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego  3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim  4. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe  5. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,  6. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.  7. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim  8. Wbudowany system pomocy w języku polskim.  9. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).  10. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące  11. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń  12. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń  13. Możliwość pracy w domenie Active Directory |
|  | Bezpieczeństwo i oprogramowanie dodatkowe – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania | Licencja min. 2 lata:  System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. 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 wrażliwości  Szyfrowanie danych:  • Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.  • Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.  Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.  Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.  Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.  Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.  Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.  Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.  Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.  Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware  Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:  • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli  • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory  • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux  • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.  • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich  • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji  Zarządzanie przez Chmurę:  1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach  2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury  3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur  4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy  5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach  6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń  7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej  Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.  Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.  1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer  2. Oprogramowanie klienckie, zarządzane z poziomu serwera.  System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:  • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie  • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD  • funkcje regulowania połączeń WiFi i Bluetooth  • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe  • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi  • funkcje blokowania dostępu dowolnemu urządzeniu  • możliwość tymczasowego dodania dostępu do urządzenia przez administratora  • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu  • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka  • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora  • możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry  • możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich  • funkcję wirtualnej klawiatury  • możliwość blokowania każdej aplikacji  • możliwość zablokowania aplikacji w oparciu o kategorie  • możliwość dodania własnych aplikacji do listy zablokowanych  • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze  • dodawanie innych aplikacji  • dodawanie aplikacji w formie portable  • możliwość wyboru pojedynczej aplikacji w konkretnej wersji  • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB  • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool  • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.  • możliwość zablokowania funkcji Printscreen  • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx  • funkcje monitorowania i kontroli przepływu poufnych informacji  • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików  • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj  • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe  • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe  • ochrona zawartości schowka systemu  • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL  • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych  • ochrona plików zamkniętych w archiwach  • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem  • możliwość tworzenia profilu DLP dla każdej polityki  • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania  • ochrona przez wyciekiem plików poprzez programy typu p2p  Monitorowanie zmian w plikach:  • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.  • Funkcje monitorowania określonych rodzajów plików.  • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.  • Generator raportów do funkcjonalności monitora zmian w plikach.  • możliwość śledzenia zmian we wszystkich plikach  • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach  • możliwość definiowana własnych typów plików  Optymalizacja systemu operacyjnego stacji klienckich:  • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku  • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem  • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich  • instruktaż stanowiskowy pracowników Zamawiającego  • dokumentacja techniczna w języku polskim  Wspierane platformy i systemy operacyjne:  1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)  2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)  3. Mac OS X, Mac OS 10  4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat  Platforma do zarządzania dla Android i iOS:   * Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę * Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.   Zarządzanie użytkownikiem   * Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email * Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika * Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi * Musi posiadać możliwość eksportu danych użytkownika   Zarządzanie urządzeniem   * Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO * Musi umożliwiać import listy urządzeń z pliku CSV * Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych * Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta * Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał * Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres * Musi zawierać podgląd aktualnie zainstalowanych aplikacji * Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, * Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł * Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres   Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:  Wymagania dotyczące technologii:   1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową 2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta. 3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:   - Microsoft Internet Explorer  - Microsoft Edge  - Mozilla Firefox  - Google Chrome  - Safari   1. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących 2. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 3. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:   - Windows 2008 R2  - Windows 2012  - Windows 2012 R2  - Windows 2016  7. Portal zarządzający musi umożliwiać:  a)           przegląd wybranych danych na podstawie konfigurowalnych widgetów  b)           zablokowania możliwości zmiany konfiguracji widgetów  c)            zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.  d)           tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności  e)           eksport wszystkich skanów podatności do pliku CSV |
| 11. | Gwarancja i wsparcie techniczne producenta | 3-letnia gwarancja producenta, Czas reakcji serwisu do końca następnego dnia roboczego. Firma serwisująca musi posiadać ISO 9001:2000 lub certyfikat równoważny na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.  Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera, dostępna w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia:  - weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa - CPU, HDD, pamięć)  Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera |
| 12 | Wymagania dodatkowe | Wbudowane porty:  • min. 1 x VGA,  • min. 1 x DVI  • min. 1 x HDMI ver. 1.4  • min. 2 x PS/2,  • min. 8 portów USB wyprowadzonych na zewnątrz komputera w tym min.: min. 2 porty USB 3.1 z przodu obudowy, 4szt. USB 3.1 z tyłu obudowy - wymagana ilość i rozmieszczenie portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, kart PCIe itp.  • porty słuchawek i mikrofonu na przednim oraz tylnym panelu obudowy.  • Komputer musi umożliwiać jego rozbudowę w postaci dedykowanych kart PCIe np. kartę WiFi a/b/g/n  • Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), PXE 2.1.  • Płyta główna posiadająca chipset rekomendowany przez producenta procesora. Zbudowana w oparciu o kondensatory polimerowe o podwyższonej trwałości., przeznaczona dla danego urządzenia; wyposażona w :   * SATA III (6 Gb/s) - 4 szt. * M.2 - 1 szt. * PCIe 3.0 x16 - 1 szt. * PCIe 2.0 x1 - 2 szt. * Złącze wyjścia S/PDIF - 1 szt. * 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM, z obsługą DDR4-3200 MHz   • Klawiatura USB w układzie polski programisty  • Mysz USB z klawiszami oraz rolką (scroll)  • Wbudowana w obudowę nagrywarka DVD +/-RW szybkość min. x24 wraz z oprogramowaniem do nagrywania i odtwarzania płyt  • Dołączony nośnik ze sterownikami   * Wsparcie dla konfiguracji RAID 0, 1, 10   Wbudowany w płytę główną układ przetwarzania energii, zapewniający możliwość całościowego zarządzania poziomem zużywanej energii poprzez wykrywanie aktualnego poziomu wykorzystania zasobów PC (CPU, GPU, HDD, zasilacza) oraz inteligentne przydzielanie mocy w czasie rzeczywistym. Układ działający automatycznie od momentu uruchomienia komputera.  Ochrona przed nadmiernym napięciem zasilania:  System zasilania chroniący obwód specjalnie zaprojektowany przez producenta płyty głównej z wbudowanymi regulatorami napięcia do ochrony chipsetu, gniazd połączeniowych i kodeków audio przed uszkodzeniem spowodowanym nieoczekiwanymi napięciami wysokiej wartości z niestabilnych albo złych zasilaczy. |
| 13. | Monitor, typ ekranu | Ekran ciekłokrystaliczny LED, IPS 21,5” |
| 14. | Jasność | 250 cd/m2 |
| 15. | Kontrast | 10 000 000:1 |
| 16. | Kąty widzenia (pion/poziom) | 178/178 stopni |
| 17. | Czas reakcji matrycy | max 1 ms |
| 18. | Rozdzielczość maksymalna | 1920 x 1080 przy 60Hz |
| 19. | Wyświetlane kolory | 16.7 milionów |
| 20. | Pochylenie | Tak |
| 21. | Powłoka powierzchni ekranu | Antyodblaskowa |
| 22. | Podświetlenie | System podświetlenia LED |
| 23. | Zużycie energii | Typowo 15W, czuwanie mniej niż 0,5W |
| 24. | Bezpieczeństwo | Monitor musi być wyposażony w tzw. Kensington Slot |
| 25. | Złącze | VGA (D-sub) - 1 szt.  HDMI - 1 szt.  Wyjście słuchawkowe - 1 szt.  Wejście audio - 1 szt. |
| 26. | Gwarancja | 3 lata gwarancji z czasem reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001:2000 lub certyfikat równoważny na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające przesłać na wezwanie zamawiającego. |
| 27. | Certyfikaty | CE |
| 28. | Inne | Wbudowane w obudowę głośniki stereo o mocy min. 2W.  Odłączana stopa, VESA 100mm |

**Poz. 15.** **Drukarka laserowa kolorowa A3– ilość szt.: 1**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
| 1 | Typ | Drukarka laserowa |
| 2 | Format | A3 |
| 3 | Drukowanie | Kolorowe, automatyczne dwustronne |
| 4 | Rozdzielczość | Min. 600x600 dpi |
| 5 | Szybkość druku | Mono: min. 26 stron/min, Kolor: Min. 26 stron/min |
| 6 | Gramatura nośników | Min. 250 g/m2 |
| 7 | Pojemność arkuszy | Min. 250 sztuk papieru |
| 8 | Łączność | USB, LAN, WIFI lub NFC |
| 9 | Miesięczne obciążenie | Min. 70 000 stron |
| 10 | Wyposażenie | Dołączone Tonery z wydajnością min. 2450 stron |
| 11 | Gwarancja | Min. 36 miesięcy |

**Poz. 16.** **Skaner– ilość szt.: 4**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
| 1 | Typ Skanera | Płaski |
| 2 | Rozdzielczość skanowania | Min. 48000 DPI |
| 3 | Głębia kolorów | Min. 48 bit |
| 4 | Obsługiwane pliki | Min. TIFF, BMP, JPEG |
| 5 | Złącza | Min. USB 2.0 |
| 6 | Gwarancja | Min. 12 miesięcy |

**Poz. 17.** **Projektor multimedialny – ilość szt.: 1**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
|  | Projektor | Multimedialny |
|  | Technologia | LCD lub Laser lub LED |
|  | Jasność | Min. 3000 ANSI |
|  | Rozdzielczość | Min. XGA 1024 x 768 |
|  | Kontrast | Min. 15 000:1 |
|  | Lampa | Min. 210W lub Laser bezlampowy |
|  | Rozmiar  projekcji (przekątna) | Min. w zakresie 30-300 cali |
|  | Złącza wbudowane | Min. VGA, HDMI, USB, RS232 |
|  | Głośniki wbudowane lub zewnętrzne | Min. 5W |
|  | Wyposażenie | Kable HDMI 10m, zasilający 5m |
|  | Gwarancja | Min. 36 miesięcy, Lampa 36 miesięcy lub 1000h |

**Poz. 18.** **Zszywacz elektryczny do papieru – ilość szt.: 2**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
| 1 | Rodzaj | Elektryczny |
| 2 | Mechanizm | Ładowanie kartek od przodu |
| 3 | Konstrukcja | Metalowa |
| 4 | Akumulator | Baterie lub zasilacz |
| 5 | Wyposażenie | 1000 zszywek |
| 6 | Gwarancja | Min. 5 lat |

**Poz. 19****. Drukarka 3D– ilość szt.: 1**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
|  | Technologia druku | Min. FFF lub FDM |
|  | Pole robocze | Min. 199 x 199 x 199 mm |
|  | Kompatybilne filamenty | Min. ABS, PLA, PETG lub PVA lub CPE |
|  | Średnica dyszy/wytłaczarki | Min. 0,4 mm |
|  | Temperatura dyszy | Min. 230 stopni |
|  | Obsługiwane typy plików | Min. STL, OBJ, 3MF lub DAE |
|  | Gwarancja | Min. 12 miesięcy |

**Poz. 20.** **Skaner 3D– ilość szt.: 1**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
| 1 | Typ | Ręczny 3D |
| 2 | Pole pomiarowe | Min. 80x80 mm |
| 3 | Rozdzielczość | Min. 1920x1080 |
| 4 | Obsługa plików | STL, PLY, OBJ |
| 5 | Rozdzielczość | Min. 1920x1080 |
| 6 | Łączność | USB 3.0 |
| 7 | Gwarancja | Min. 12 miesięcy |

**Poz. 21.** **Bindownica– ilość szt.: 1**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj** | **Wymagane minimalne parametry** |
| 1 | Typ | Ręczna do grzbietów plastikowych |
| 2 | Dźwignia | Osobna dźwignia do dziurkowania, osobna dźwignia do otwierania grzbietów |
| 3 | Wskaźnik | Czytelny do doboru grzbietu do ilości dziurkowanych kartek |
| 4 | Dziurkowanie | Jednorazowo do min. 20 arkuszy papieru |
| 5 | Gwarancja | Min. 2 lata |