**Załącznik 3 do SWZ**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**Zakup komputerów i laptopów w ramach realizacji projektu grantowego „Cyfrowa Gmina”**

1. **Stacje robocze – Typ I - 3 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| Typ | Komputer stacjonarny.  |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej |
| Wydajność | Oferowany komputer musi osiągać w teście wydajności SYSMARK 25 Overall Rating, wynik 1700 pkt. **Wydruk wydajności należy załączyć do oferty.** Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS ( tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). |
| Pamięć RAM | 16GB DDR4 3200 MHz. Możliwość rozbudowy do 128 GB. Cztery słoty na pamięć RAM; |
| Pamięć masowa | Dysk 500GB SSD PCIeKomputer musi umożliwiać instalację 3 HDD, dopuszcza się konfigurację dysk M.2 + 2 dyski magnetyczne |
| Grafika | Dwie karty graficzne osiągające w teście PassMark 3D Graphics Mark wyniki 1900 i 8900 pkt.**Załączyć do oferty wydruki ze stron** [**https://www.videocardbenchmark.net**](https://www.videocardbenchmark.net) **lub** [**https://www.passmark.com**](https://www.passmark.com) |
| Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik 2W w obudowie komputera, port słuchawek i mikrofonu na przednim panelu (dopuszcza się rozwiązanie port combo), na tylnym panelu złącze audio out. Czytnik kart multimedialnych czytający karty SD 4.0 |
| Obudowa | Typu MT z obsługą kart PCI Express o wysokim profilu, wyposażona w wewnętrzną wnękę 2,5” lub 3,5”;Napęd optyczny w dedykowanej wnęce zewnętrznej;Obudowa fabrycznie przystosowana do pracy w orientacji pionowej i poziomej wyposażona w dystanse gumowe zapobiegające poślizgom obudowy i zarysowaniu lakieru. Nie dopuszcza się aby w bocznych ściankach obudowy były usytuowane otwory wentylacyjne. Cyrkulacja powietrza tylko przez przedni i tylny panel z zachowaniem ruchu powietrza przód -> tył. Suma wymiarów obudowy nie może przekraczać 100 cm; Zasilacz o mocy 400W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności 90% przy obciążeniu zasilacza na poziomie 50% oraz o 85% przy obciążeniu zasilacza na poziomie 100%,Obudowa musi pozwalać na demontaż kart rozszerzeń, napędu optycznego, dysku 3,5” oraz 2,5” bez konieczności użycia narzędzi - wyklucza się użycie wkrętów, śrub motylkowych, śrub radełkowych;Musi posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym;Musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki;Musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami. Sygnalizacja oparta na zmianie statusów diody LED. W szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię CMOS baterii, awarię BIOS’u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. |
| Bezpieczeństwo | TPM zintegrowany z płyta główną; System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. |
| Zdalne zarządzanie | Technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca:* monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej;
* zdalną konfigurację ustawień BIOS,
* zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego;
* zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej.
* technologia zarządzania i monitorowania komputera na poziomie sprzętowym musi być zgodna z otwartymi standardami DMTF WS-MAN (http://www.dmtf.org/standards/wsman) oraz DASH (http://www.dmtf.org/standards/mgmt/dash/).
 |
| BIOS | BIOS zgodny ze specyfikacją UEFI; Pełna obsługa BIOS za pomocą myszy bez używania klawiatury;Informacje dostępne z poziomu BIOS na potrzeby inwentaryzacji: wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach, procesor (typ, nazwa, typowa prędkość, minimalna, maksymalna, cache L2 i L3) , pojemności zainstalowanego lub zainstalowanych dysków twardych, MAC adres karty sieciowej, kontroler audio. Informacje muszą być dostępne w samym menu BIOS bez stosowania dodatkowego oprogramowania jak i wbudowanego systemu diagnostycznego.Możliwość, ustawienia hasła na poziomie:- administratora;- użytkownika, umożliwiające użytkownikowi zmianę hasła zgodnie z uprawnieniami nadanymi przez administratora;Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.Możliwość wyłączenia/włączenia karty sieciowej, kontrolera SATA w tym również pojedynczo, kontrolera audio, układu TPM, czujnika otwarcia obudowy lub ustawienia go w tryb cichy Możliwość przypisania w BIOS numeru nadawanego przez administratora oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym;Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.Możliwość wyłączania portów USB w szczególności pojedynczo w dowolnej kombinacji. BIOS musi nanosić automatycznie wszystkie zmiany konfiguracji dotyczące pamięci, procesora, dysku. |
| Wirtualizacja | Sprzętowe wsparcie wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu;Możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu; |
| Certyfikaty i standardy | Certyfikat TCO, wymagana certyfikacja na stronie: <https://tcocertified.com/pl/> – **załączyć do oferty wydruk ze strony** |
| Wbudowane porty i wyposażenie  | 2 x DisplayPort1 x HDMI 2.01 x LAN 10/100/1000 wspierająca obsługęWoL, umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem;Porty USB 10 szt., z czego 4 szt. na panelu przednim, w tym 2 szt. USB 3.2, w tym 1 szt. USB typu C;Wymagana ilość i rozmieszczenie na zewnątrz obudowy komputera wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Wszystkie wymagane porty mają być w sposób stały zintegrowane z obudową;Płyta główna wyposażona w :1 slot PCI Express x16 Gen.3, 1 slot PCI Express x44 złącza UDIMM z obsługą do 128GB DDR4 pamięci RAM, 3 złącza SATA w tym 2 szt. SATA 3.0; 1 złącze M.2 dedykowane dla syków SSD1 złącze M.2 WLANKlawiatura USB w układzie polski programisty Mysz laserowa USB z rolką (scroll) Nagrywarka DVD +/-RW o prędkości min. 8x  |
| Wsparcie techniczne  | Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia danych o urządzeniu na jednej witrynie internetowej producenta, w tym co najmniej: automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego; |
| Warunki gwarancji i serwisu | 3-letnia gwarancja producenta świadczona na miejscu u klientaCzas reakcji serwisu - do końca następnego dnia roboczego.Serwis musi być świadczony zgodnie normami ISO 27001 **– załączyć do oferty certyfikat dla oferenta;** |
| System operacyjny | System operacyjny Windows 10 PRO lub 11 PRO 64bit lub równoważny klasy PC spełniający następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
2. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
3. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych
4. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego
5. Interfejs użytkownika dostępny w języku polskim i angielskim
6. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.
7. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe
8. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego;
9. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
10. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
11. Graficzne środowisko instalacji i konfiguracji w języku polskim
12. Wbudowany system pomocy w języku polskim.
13. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
14. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego.
15. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
16. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
17. Zabezpieczony hasłem hierarchiczny dostęp do systemu;
18. Konta i profile użytkowników zarządzane zdalnie;
19. Praca systemu w trybie ochrony kont użytkowników.
20. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze;
21. Możliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
22. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika
23. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
24. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
25. Oprogramowanie dla tworzenia kopii zapasowych (Backup);
26. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
27. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
28. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
29. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);
30. Wbudowany mechanizm wirtualizacji typu hypervisor;
31. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego.
32. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego.
33. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych;
34. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
35. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny;
36. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików;
37. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików.
38. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi.
39. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne;
40. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM
41. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych;
42. Możliwość tworzenia wirtualnych kart inteligentnych.
43. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)
44. Wsparcie dla IPSEC oparte na politykach;
45. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
46. Mechanizmy logowania w oparciu o:
47. Login i hasło,
48. Karty inteligentne i certyfikaty (smartcard),
49. Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM;
50. Umożliwiający pracę w domenie;
 |
| Oprogramowanie użytkowe | System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance + musi umożliwiać co najmniej:1. Wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,
2. Wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,
3. Stosowanie kwarantanny
4. Wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)
5. Skanowanie urządzeń USB natychmiast po podłączeniu,
6. Automatyczne odłączanie zainfekowanej końcówki od sieci,
7. Skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji.
8. Zarządzanie stacją kliencką poprzez zbieranie informacji co najmniej o: nazwie, 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 (procesor, RAM, SN, dysk), BIOS, interfejsach sieciowych, dołączonych peryferiach.
9. Musi posiadać moduł ochrony IDS/IPS
10. Musi posiadać mechanizm wykrywania skanowania portów
11. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów
12. Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości
13. Oprogramowanie do szyfrowania, chroniące dane na stacji za pomocą algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH.
14. Pełne szyfrowanie dysków działających w oferowanych komputerach zapobiegające utracie danych z powodu utraty / kradzieży stacji roboczej.
15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak pendrive, dyski USB i udostępniać ją tylko autoryzowanym użytkownikom.
16. Musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji;
17. Musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji.
18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB oraz możliwości uruchamiania oprogramowania z takich dysków. Blokada ta musi umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.
19. Interfejs zarządzania musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji.
20. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware poprzez ograniczenie możliwości modyfikowania chronionych plików, tylko do procesów systemowych oraz zaufanych aplikacji.
21. Możliwość zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika.
22. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych ochroną any ransomware.
23. Monitorowanie krytycznych danych użytkownika zapobiegające atakom ransomware;
24. Centralna konsola zarządzająca umożliwiająca co najmniej:
25. przechowywanie danych w bazie typu SQL
26. zdalną instalację lub deinstalację oprogramowania, na pojedynczych stacjach, zakresie adresów IP lub grupie z ActiveDirectory;
27. tworzenie paczek instalacyjnych oprogramowania, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi oraz formatach dla systemów Linux
28. centralną dystrybucję uaktualnień definicji ochronnych, których źródłem będzie plik na serwerze konsoli;
29. raportowanie z prezentacją tabelaryczną i graficzną, możliwością automatycznego czyszczenia starych raportów, eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich;
30. definiowanie struktury opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji;
31. Możliwość tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera;
32. Dostęp do konsoli z dowolnego miejsca w nagłych przypadkach;
33. Możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń
34. 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.
35. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych;
36. System musi umożliwiać, z konsoli na serwerze, co najmniej:
37. różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie
38. przyznawanie praw dostępu dla nośników pamięci tj. USB, CD
39. regulowania połączeń WiFi i Bluetooth
40. kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe
41. blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi
42. blokowanie dostępu dowolnemu urządzeniu
43. tymczasowe dodanie dostępu do urządzenia przez administratora
44. szyfrowanie zawartości USB i udostępnianie jej na stacjach końcowych;
45. zablokowanie funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka
46. zezwalać na dostęp tylko urządzeniom wcześniej dodanym przez administratora
47. używania tylko zaufanych urządzeń sieciowych;
48. Funkcja wirtualnej klawiatury
49. Możliwość blokowania każdej aplikacji , w tym w oparciu o kategorie
50. Możliwość dodania własnych aplikacji do listy zablokowanych
51. Tworzenie listy aplikacji zainstalowanych na komputerach klientach poprzez konsolę administracyjną na serwerze
52. Kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool
53. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki;
54. Możliwość zablokowania funkcji Printscreen
55. Monitorowanie przesyłu danych między aplikacjami;
56. Monitorowanie i kontrola przepływu poufnych informacji
57. Blokowanie plików w oparciu o ich rozszerzenie lub rodzaj
58. Monitorowanie i zarządzanie danymi udostępnianymi poprzez zasoby sieciowe;
59. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe
60. Ochrona zawartości schowka systemu
61. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL
62. Dodawanie wyjątków dla domen, aplikacji i lokalizacji sieciowych
63. Ochrona plików zamkniętych w archiwach
64. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem
65. Możliwość tworzenia profilu DLP dla każdej polityki
66. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania
67. Ochrona przez wyciekiem plików poprzez programy typu p2p
68. Monitorowanie działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.
69. Monitorowanie określonych rodzajów plików.
70. Możliwość wykluczenia określonych plików/folderów z procedury monitorowania.
71. Możliwość śledzenia zmian we wszystkich plikach
72. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na stacjach roboczych;
73. Możliwość definiowana własnych typów plików
74. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku
75. Optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem
76. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich
77. System ochrony i zarządzania urządzeniami za pomocą platformy w chmurze;.
78. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi
79. Musi posiadać możliwość eksportu danych użytkownika
80. Import listy urządzeń z pliku CSV
81. Dodawanie urządzeń;
82. Podgląd co najmniej następujących informacji konfiguracji: data i status wdrożenia, status urządzenia, numer telefonu, właściciel, grupa, reguły, wersja agenta
83. Podgląd co najmniej następujących informacji sprzętowych: model, producent, system, adres MAC, bluetooth, wolna przestrzeń na dysku, całkowita przeszłość na dysku, użycie procesora;
84. Podgląd zainstalowanych aplikacji;
85. Moduł raportowania aktywności, skanowania oraz naruszenia reguł;
86. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa dostępne przez przeglądarkę internetową;
87. Portal zarządzający w postaci SaaS;
88. Skanowanie podatności za pomocą nodów skanujących;
89. Nody skanujące w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie
90. Portal zarządzający musi umożliwiać:
91. przegląd wybranych danych;
92. zablokowanie możliwości zmiany konfiguracji;
93. zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów;
94. tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności
95. eksport skanów podatności do pliku CSV;
96. Deduplikacja danych na źródle,
97. Backup przyrostowy i różnicowy,
98. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,
99. Backup danych lokalnych – plikowy oraz poczty;
100. Backup otwartych plików;
101. Filtr plików oraz folderów,
102. Domyślne wykluczenia zbędnych plików;
103. Wyłączanie komputera po wykonaniu backup;
104. Przywracanie danych do wskazanej lokalizacji,
105. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,
106. Wyszukiwanie plików w repozytorium użytkownika,
107. Automatyczne logowanie,
108. Zapamiętywanie danych logowania,
109. Automatyczne uruchamianie programu przy starcie systemu,
110. Ustawianie priorytetu dla procesu backupu,
111. Zmiana klucza szyfrującego,
112. Ustawienia przepustowości/zajętości pasma,
113. Konfiguracja wydajności procesu backupu,
114. Zastępowanie nazwy pliku GUID-em,
115. Szyfrowanie danych algorytmem AES 256 CBC;
116. Kompresja danych,
117. Deklaracja klucza szyfrującego dane użytkownika,
118. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,
119. Obliczanie sumy kontrolnej,
120. Licencje z przestrzenią w chmurze –50 GB.
121. Wsparcie techniczne, świadczone przez producenta, w języku polskim;
122. **U**pgrade i instalację wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,
123. Sprawdzenie przed instalacją każdego sterownika, aplikacji, BIOS’u bezpośrednio na stronie producenta, a w szczególności uzyskanie informacji o:
	* poprawkach i usprawnieniach dotyczących aktualizacji
	* dacie wydania aktualizacji
	* priorytecie aktualizacji
	* zgodności z systemem operacyjnym
	* jakiego komponentu sprzętu dotyczy aktualizacja
	* wszystkich poprzednich aktualizacjach z informacjami jak powyżej;
124. Uzyskanie listy najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne
125. Włączenie/wyłączenie funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika lub aplikacji;
126. Rozpoznanie modelu oferowanego komputera, numeru seryjnego, informację kiedy dokonany został ostatnio upgrade;
127. Sprawdzenia historii upgradeów z informacją jakie sterowniki były instalowane z dokładną datą i wersją;
128. Wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji;
129. Wygenerowanie raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją jakich komponentów dotyczyły oraz błędach podczas instalowania. Raport musi zawierać z datą ( dd-mm-rrrr ) i godzinę podjętych i wykonanych akcji.w okresie co najmniej roku wstecz.
 |

**Monitor – 3 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| Rozmiar  |  27 cali; |
| Podświetlenie | LED |
| Typ panelu | Przeciwodblaskowy, IPS; |
| Format obrazu | 16:9 |
| Rozdzielczość | 1920 x 1080 |
| Czas reakcji matrycy | Maksymalnie 8 ms. |
| Jasność | 300  cd/m² |
| Kontrast statyczny | 1000:1 |
| Plamka | Maksymalnie 0,32 mm |
| Kat nachylenia | -5 do 20 stopni |
| Regulacja wysokości | 0 do 100 mm; |
| Katy widzenia | * 178 stopni;
 |
| Złącza | 1 x VGA, 1 x HDMI, 1 x DisplayPort 1.2; |
| Pobór mocy podczas pracy | Maksymalnie 18W; |
| Warunki gwarancji | 3 lata; |
| Wymagania dodatkowe | Wbudowane głośniki, zgodność ze standardem VESA, gniazdo blokady bezpieczeństwa, kabel HDMI i VGA, zgodność ze standardem EnergyStar; |

1. **Stacje robocze – Typ II - 17 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| Typ | Komputer stacjonarny.  |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej |
| Wydajność | Oferowany komputer musi osiągać w teście wydajności SYSMARK 25 Overall Rating, wynik 1600 pkt. **Wydruk wydajności należy załączyć do oferty.** Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS ( tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). |
| Pamięć RAM | 16GB DDR4 3200 MHz. Możliwość rozbudowy do 128 GB. Cztery sloty na pamięć RAM; |
| Pamięć masowa | Dysk 500GB SSD PCIeKomputer musi umożliwiać instalację 3 HDD, dopuszcza się konfigurację dysk M.2 + 2 dyski magnetyczne |
| Grafika | Zintegrowana z procesorem, musi osiągać w teście PassMark 3D Graphics Mark wynik 1900.**Załączyć do oferty wydruki ze stron** [**https://www.videocardbenchmark.net**](https://www.videocardbenchmark.net) **lub** [**https://www.passmark.com**](https://www.passmark.com) |
| Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik 2W w obudowie komputera, port słuchawek i mikrofonu na przednim panelu (dopuszcza się rozwiązanie port combo), na tylnym panelu złącze audio out. Czytnik kart multimedialnych czytający karty SD 4.0 |
| Obudowa | Typu SFF z obsługą kart PCI Express wyłącznie o niskim profilu, wyposażona w wewnętrzną wnękę 2,5” lub 3,5”;Napęd optyczny w dedykowanej wnęce zewnętrznej;Obudowa fabrycznie przystosowana do pracy w orientacji pionowej i poziomej wyposażona w dystanse gumowe zapobiegające poślizgom obudowy i zarysowaniu lakieru. Nie dopuszcza się aby w bocznych ściankach obudowy były usytuowane otwory wentylacyjne. Cyrkulacja powietrza tylko przez przedni i tylny panel z zachowaniem ruchu powietrza przód -> tył. Suma wymiarów obudowy nie może przekraczać 70cm; Zasilacz o mocy 300W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności 90% przy obciążeniu zasilacza na poziomie 50% oraz o 85% przy obciążeniu zasilacza na poziomie 100%,Obudowa musi pozwalać na demontaż kart rozszerzeń, napędu optycznego, dysku 3,5” oraz 2,5” bez konieczności użycia narzędzi - wyklucza się użycie wkrętów, śrub motylkowych, śrub radełkowych;Musi posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym;Musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki;Musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami. Sygnalizacja oparta na zmianie statusów diody LED. W szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię CMOS baterii, awarię BIOS’u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Komputer musi być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. |
| Bezpieczeństwo | TPM zinegrowany z płyta główną; System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. |
| Zdalne zarządzanie | Technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca:* monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej;
* zdalną konfigurację ustawień BIOS,
* zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM lub FDD z serwera zarządzającego;
* zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji (wersja, zainstalowane uaktualnienia, sygnatury wirusów, itp.) z wbudowanej pamięci nieulotnej.
* technologia zarządzania i monitorowania komputera na poziomie sprzętowym musi być zgodna z otwartymi standardami DMTF WS-MAN (http://www.dmtf.org/standards/wsman) oraz DASH (http://www.dmtf.org/standards/mgmt/dash/).
 |
| BIOS | BIOS zgodny ze specyfikacją UEFI; Pełna obsługa BIOS za pomocą myszy bez używania klawiatury;Informacje dostępne z poziomu BIOS na potrzeby inwentaryzacji: wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach, procesor (typ, nazwa, typowa prędkość, minimalna, maksymalna, cache L2 i L3) , pojemności zainstalowanego lub zainstalowanych dysków twardych, MAC adres karty sieciowej, kontroler audio. Informacje muszą być dostępne w samym menu BIOS bez stosowania dodatkowego oprogramowania jak i wbudowanego systemu diagnostycznego.Możliwość, ustawienia hasła na poziomie:- administratora;- użytkownika, umożliwiające użytkownikowi zmianę hasła zgodnie z uprawnieniami nadanymi przez administratora;Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.Możliwość wyłączenia/włączenia karty sieciowej, kontrolera SATA w tym również pojedynczo, kontrolera audio, układu TPM, czujnika otwarcia obudowy lub ustawienia go w tryb cichy Możliwość przypisania w BIOS numeru nadawanego przez administratora oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym;Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.Możliwość wyłączania portów USB w szczególności pojedynczo w dowolnej kombinacji. BIOS musi nanosić automatycznie wszystkie zmiany konfiguracji dotyczące pamięci, procesora, dysku. |
| Wirtualizacja | Sprzętowe wsparcie wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu;Możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu; |
| Certyfikaty i standardy | Certyfikat TCO, wymagana certyfikacja na stronie: <https://tcocertified.com/pl/> – **załączyć do oferty wydruk ze strony** |
| Wbudowane porty i wyposażenie | 2 x DisplayPort1 x HDMI 2.01 x LAN 10/100/1000 wspierająca obsługęWoL, umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem;Porty USB 10 szt., z czego 4 szt. na panelu przednim, w tym 2 szt. USB 3.2, w tym 1 szt. USB typu C;Wymagana ilość i rozmieszczenie na zewnątrz obudowy komputera wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Wszystkie wymagane porty mają być w sposób stały zintegrowane z obudową;Płyta główna wyposażona w :1 slot PCI Express x16 Gen.3, 1 slot PCI Express x44 złącza UDIMM z obsługą do 128GB DDR4 pamięci RAM, 3 złącza SATA w tym 2 szt. SATA 3.0; 1 złącze M.2 dedykowane dla syków SSD1 złącze M.2 WLANKlawiatura USB w układzie polski programisty Mysz laserowa USB z rolką (scroll) Nagrywarka DVD +/-RW o prędkości min. 8x  |
| Wsparcie techniczne  | Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia danych o urządzeniu na jednej witrynie internetowej producenta, w tym co najmniej: automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego; |
| Warunki gwarancji i serwisu | 3-letnia gwarancja producenta świadczona na miejscu u klientaCzas reakcji serwisu - do końca następnego dnia roboczegoSerwis musi być świadczony zgodnie normą i ISO 27001 **– załączyć do oferty certyfikaty dla oferenta;** |
| System operacyjny | System operacyjny Windows 10 PRO lub 11 PRO 64bit lub równoważny klasy PC spełniający następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
2. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
3. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych
4. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego
5. Interfejs użytkownika dostępny w języku polskim i angielskim
6. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.
7. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe
8. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego;
9. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
10. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
11. Graficzne środowisko instalacji i konfiguracji w języku polskim
12. Wbudowany system pomocy w języku polskim.
13. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
14. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego.
15. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
16. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
17. Zabezpieczony hasłem hierarchiczny dostęp do systemu;
18. Konta i profile użytkowników zarządzane zdalnie;
19. Praca systemu w trybie ochrony kont użytkowników.
20. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze;
21. Możliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
22. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika
23. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
24. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
25. Oprogramowanie dla tworzenia kopii zapasowych (Backup);
26. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
27. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
28. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
29. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);
30. Wbudowany mechanizm wirtualizacji typu hypervisor;
31. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego.
32. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego.
33. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych;
34. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
35. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny;
36. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików;
37. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików.
38. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi.
39. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne;
40. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM
41. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych;
42. Możliwość tworzenia wirtualnych kart inteligentnych.
43. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)
44. Wsparcie dla IPSEC oparte na politykach;
45. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
46. Mechanizmy logowania w oparciu o:
47. Login i hasło,
48. Karty inteligentne i certyfikaty (smartcard),
49. Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM;
50. Umożliwiający pracę w domenie;
 |
| Oprogramowanie użytkowe | System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance + musi umożliwiać co najmniej:1. Wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,
2. Wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,
3. Stosowanie kwarantanny
4. Wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)
5. Skanowanie urządzeń USB natychmiast po podłączeniu,
6. Automatyczne odłączanie zainfekowanej końcówki od sieci,
7. Skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji.
8. Zarządzanie stacją kliencką poprzez zbieranie informacji co najmniej o: nazwie, 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 (procesor, RAM, SN, dysk), BIOS, interfejsach sieciowych, dołączonych peryferiach.
9. Musi posiadać moduł ochrony IDS/IPS
10. Musi posiadać mechanizm wykrywania skanowania portów
11. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów
12. Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości
13. Oprogramowanie do szyfrowania, chroniące dane na stacji za pomocą algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH.
14. Pełne szyfrowanie dysków działających w oferowanych komputerach zapobiegające utracie danych z powodu utraty / kradzieży stacji roboczej.
15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak pendrive, dyski USB i udostępniać ją tylko autoryzowanym użytkownikom.
16. Musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji;
17. Musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji.
18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB oraz możliwości uruchamiania oprogramowania z takich dysków. Blokada ta musi umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.
19. Interfejs zarządzania musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji.
20. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware poprzez ograniczenie możliwości modyfikowania chronionych plików, tylko do procesów systemowych oraz zaufanych aplikacji.
21. Możliwość zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika.
22. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych ochroną any ransomware.
23. Monitorowanie krytycznych danych użytkownika zapobiegające atakom ransomware;
24. Centralna konsola zarządzająca umożliwiająca co najmniej:
25. przechowywanie danych w bazie typu SQL
26. zdalną instalację lub deinstalację oprogramowania, na pojedynczych stacjach, zakresie adresów IP lub grupie z ActiveDirectory;
27. tworzenie paczek instalacyjnych oprogramowania, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi oraz formatach dla systemów Linux
28. centralną dystrybucję uaktualnień definicji ochronnych, których źródłem będzie plik na serwerz konsoli;
29. raportowanie z prezentacją tabelaryczną i graficzną, możliwością automatycznego czyszczenia starych raportów, eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich;
30. definiowanie struktury opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji;
31. Możliwość tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera;
32. Dostęp do konsoli z dowolnego miejsca w nagłych przypadkach;
33. Możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń
34. 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.
35. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych;
36. System musi umożliwiać, z konsoli na serwerze, co najmniej:
37. różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie
38. przyznawanie praw dostępu dla nośników pamięci tj. USB, CD
39. regulowania połączeń WiFi i Bluetooth
40. kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe
41. blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi
42. blokowanie dostępu dowolnemu urządzeniu
43. tymczasowe dodanie dostępu do urządzenia przez administratora
44. szyfrowanie zawartości USB i udostępnianie jej na stacjach końcowych;
45. zablokowanie funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka
46. zezwalać na dostęp tylko urządzeniom wcześniej dodanym przez administratora
47. używana tylko zaufanych urządzeń sieciowych;
48. Funkcja wirtualnej klawiatury
49. Możliwość blokowania każdej aplikacji , w tym w oparciu o kategorie
50. Możliwość dodania własnych aplikacji do listy zablokowanych
51. Tworzenie listy aplikacji zainstalowanych na komputerach klientach poprzez konsolę administracyjną na serwerze
52. Kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool
53. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki;
54. Możliwość zablokowania funkcji Printscreen
55. Monitorowanie przesyłu danych między aplikacjami;
56. Monitorowanie i kontrola przepływu poufnych informacji
57. Blokowanie plików w oparciu o ich rozszerzenie lub rodzaj
58. Monitorowanie i zarządzanie danymi udostępnianymi poprzez zasoby sieciowe;
59. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe
60. Ochrona zawartości schowka systemu
61. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL
62. Dodawanie wyjątków dla domen, aplikacji i lokalizacji sieciowych
63. Ochrona plików zamkniętych w archiwach
64. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem
65. Możliwość tworzenia profilu DLP dla każdej polityki
66. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania
67. Ochrona przez wyciekiem plików poprzez programy typu p2p
68. Monitorowanie działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.
69. Monitorowanie określonych rodzajów plików.
70. Możliwość wykluczenia określonych plików/folderów z procedury monitorowania.
71. Możliwość śledzenia zmian we wszystkich plikach
72. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na stacjach roboczych;
73. Możliwość definiowana własnych typów plików
74. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku
75. Optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem
76. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich
77. System ochrony i zarządzania urządzeniami za pomocą platformy w chmurze;.
78. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi
79. Musi posiadać możliwość eksportu danych użytkownika
80. Import listy urządzeń z pliku CSV
81. Dodawanie urządzeń;
82. Podgląd co najmniej następujących informacji konfiguracji: data i status wdrożenia, status urządzenia, numer telefonu, właściciel, grupa, reguły, wersja agenta
83. Podgląd co najmniej następujących informacji sprzętowych: model, producent, system, adres MAC, bluetooth, wolna przestrzeń na dysku, całkowita przeszłość na dysku, użycie procesora,;
84. Podgląd zainstalowanych aplikacji;
85. Moduł raportowania aktywności, skanowania oraz naruszenia reguł;
86. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa dostępne przez przeglądarkę internetową;
87. Portal zarządzający w postaci SaaS;
88. Skanowanie podatności za pomocą nodów skanujących;
89. Nody skanujące w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie
90. Portal zarządzający musi umożliwiać:
91. przegląd wybranych danych;
92. zablokowanie możliwości zmiany konfiguracji;
93. zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów;
94. tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności
95. eksport skanów podatności do pliku CSV;
96. Deduplikacja danych na źródle,
97. Backup przyrostowy i różnicowy,
98. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,
99. Backup danych lokalnych – plikowy oraz poczty;
100. Backup otwartych plików;
101. Filtr plików oraz folderów,
102. Domyślne wykluczenia zbędnych plików;
103. Wyłączanie komputera po wykonaniu backup;
104. Przywracanie danych do wskazanej lokalizacji,
105. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,
106. Wyszukiwanie plików w repozytorium użytkownika,
107. Automatyczne logowanie,
108. Zapamiętywanie danych logowania,
109. Automatyczne uruchamianie programu przy starcie systemu,
110. Ustawianie priorytetu dla procesu backupu,
111. Zmiana klucza szyfrującego,
112. Ustawienia przepustowości/zajętości pasma,
113. Konfiguracja wydajności procesu backupu,
114. Zastępowanie nazwy pliku GUID-em,
115. Szyfrowanie danych algorytmem AES 256 CBC;
116. Kompresja danych,
117. Deklaracja klucza szyfrującego dane użytkownika,
118. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,
119. Obliczanie sumy kontrolnej,
120. Licencje z przestrzenią w chmurze –50 GB.
121. Wsparcie techniczne, świadczone przez producenta, w języku polskim;
122. **U**pgrade i instalację wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,
123. Sprawdzenie przed instalacją każdego sterownika, aplikacji, BIOS’u bezpośrednio na stronie producenta, a w szczególności uzyskanie informacji o:
	* poprawkach i usprawnieniach dotyczących aktualizacji
	* dacie wydania aktualizacji
	* priorytecie aktualizacji
	* zgodności z systemem operacyjnym
	* jakiego komponentu sprzętu dotyczy aktualizacja
	* wszystkich poprzednich aktualizacjach z informacjami jak powyżej;
124. Uzyskanie listy najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne
125. Włączenie/wyłączenie funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika lub aplikacji;
126. Rozpoznanie modelu oferowanego komputera, numeru seryjnego, informację kiedy dokonany został ostatnio upgrade;
127. Sprawdzenia historii upgradeów z informacją jakie sterowniki były instalowane z dokładną datą i wersją;
128. Wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji;
129. Wygenerowanie raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją jakich komponentów dotyczyły oraz błędach podczas instalowania. Raport musi zawierać z datą ( dd-mm-rrrr ) i godzinę podjętych i wykonanych akcji w okresie co najmniej roku wstecz.
 |

**Monitor – 17 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| Rozmiar  |  23,8 cala; |
| Podświetlenie | LED |
| Typ panelu | Przeciwodblaskowy, IPS, TFT; |
| Format obrazu | 16:9 |
| Rozdzielczość | 1920 x 1080 |
| Czas reakcji matrycy | Maksymalnie 8 ms. |
| Jasność | 250  cd/m² |
| Kontrast statyczny | 1000:1 |
| Plamka | Maksymalnie 0,28 mm |
| Kat nachylenia | -5 do 20 stopni |
| Katy widzenia | * 178 stopni;
 |
| Złącza | 1 x VGA, 1 x DisplayPort 1.2; |
| Pobór mocy podczas pracy | Maksymalnie 30W; |
| Warunki gwarancji | 3 lata; |
| Wymagania dodatkowe | Zgodność ze standardem VESA, gniazdo blokady bezpieczeństwa, kabel DP i VGA, zgodność ze standardem EnergyStar; |

1. **Laptopy - 5 szt.**

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej |
| Wydajność | Oferowany komputer musi osiągać w teście wydajności SYSMARK 25 Overall Rating, wynik 1200 pkt. **Wydruk wydajności należy załączyć do oferty.**Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzaniach. Nie dopuszcza się stosowanie overclokingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS ( tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). |
| Pamięć RAM | 16GB DDR4 2400MHz, możliwość rozbudowy do 32GB, 2 sloty na pamięci w tym jeden wolny. |
| Pamięć masowa | Dysk 512GB NVMe SSD M.2Komputer musi umożliwiać montaż dwóch dysków w konfiguracji M.2 + 2,5” |
| Grafika | Musi osiągać w teście PassMark 3D Graphics Mark wynik 3300. **Załączyć do oferty wydruki ze stron** [**https://www.videocardbenchmark.net**](https://www.videocardbenchmark.net) **lub** [**https://www.passmark.com**](https://www.passmark.com) |
| Klawiatura | Klawiatura z podświetleniem, układ US;Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12. |
| Multimedia | Karta dźwiękowa zintegrowana z płytą główną;Wbudowane głośniki stereo 2 x 2W;Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy. Kamera internetowa z diodą informującą o aktywności, 720p, trwale zainstalowana w obudowie matrycy.Czytnik kart microSD;1 port audio typu combo (słuchawki i mikrofon) |
| Łączność bezprzewodowa | Wi-Fi 6 AX201 2x2 + Bluetooth 5.1  |
| Bateria i zasilanie | 3-komorowa 40Whr umożliwiająca szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin.Czas pracy na baterii - 8 godzin.Zasilacz o mocy min. 65W |
| Waga i wymiary | Waga- maksymalnie 2 kg z baterią |
| BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI;Pełna obsługa za pomocą klawiatury i urządzenia wskazującego wmontowanego na stałe oraz samego urządzenia wskazującego;Możliwość, bez uruchamiania systemu operacyjnego, odczytania z BIOS informacji o: dacie produkcji komputera, kontrolerze audio, procesorze, a w szczególności osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach;Niezmazywalne i nieedytowalne pole asset tag;Możliwość ustawienia hasła dla administratora;Możliwość ustawienia hasła dla użytkownika które jednocześnie będzie blokować uruchamianie systemu z jakichkolwiek urządzeń;Możliwość konfiguracji zależności między tymi hasłami;Hasła muszą umożliwiać zawarcie w sobie znaków specjalnych, liczb i liter;Możliwość odczytania informacji o stanie naładowania baterii, podpiętego zasilacza, zarządzanie trybem ładowania baterii;Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania i konieczności aktualizacji BIOS.Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym; |
| Certyfikaty | Certyfikat TCO, wymagana certyfikacja na stronie <https://tcocertified.com> – **załączyć do oferty wydruk ze strony;** |
| Porty i złącza | Wbudowane porty i złącza: 1x HDMI 1.41x RJ-45, 2x USB 3.1,1x USB 3.1 TYP-C z obsługą DP 1.21x USB 2.0port zasilania, złącze linki zabezpieczającą.Złącze do podłączenia stacji dokującej umożliwiające ładowanie laptopa.  |
| Diagnostyka | System diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. Pełna funkcjonalność systemu diagnostycznego musi być realizowana bez użycia dostępu do sieci LAN, internetu, dysku twardego, również w przypadku jego braku, urządzeń zewnętrznych i wewnętrznych typu : pamięć flash; |
| Bezpieczeństwo | Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej. |
| Wsparcie techniczne  | Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia danych o urządzeniu na jednej witrynie internetowej producenta, w tym co najmniej: automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego; |
| Warunki gwarancji i serwisu | 3-letnia gwarancja świadczona na miejscu u klientaCzas reakcji serwisu - do końca następnego dnia roboczego.Serwis musi być świadczony zgodnie normami ISO 27001 **– załączyć do oferty certyfikat dla oferenta;** |
| System operacyjny | System operacyjny Windows 10 PRO lub 11 PRO 64bit lub równoważny klasy PC spełniający następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
2. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
3. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych
4. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego
5. Interfejs użytkownika dostępny w języku polskim i angielskim
6. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.
7. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe
8. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z poziomów: menu, otwartego okna systemu operacyjnego;
9. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
10. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.
11. Graficzne środowisko instalacji i konfiguracji w języku polskim
12. Wbudowany system pomocy w języku polskim.
13. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
14. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego.
15. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.
16. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.
17. Zabezpieczony hasłem hierarchiczny dostęp do systemu;
18. Konta i profile użytkowników zarządzane zdalnie;
19. Praca systemu w trybie ochrony kont użytkowników.
20. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze;
21. Możliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".
22. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na serwerze plików z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika
23. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
24. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
25. Oprogramowanie dla tworzenia kopii zapasowych (Backup);
26. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
27. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
28. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.
29. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);
30. Wbudowany mechanizm wirtualizacji typu hypervisor;
31. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego.
32. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego.
33. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych;
34. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
35. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny;
36. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików;
37. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików.
38. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi.
39. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne;
40. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM
41. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych;
42. Możliwość tworzenia wirtualnych kart inteligentnych.
43. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)
44. Wsparcie dla IPSEC oparte na politykach;
45. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
46. Mechanizmy logowania w oparciu o:
47. Login i hasło,
48. Karty inteligentne i certyfikaty (smartcard),
49. Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM;
50. Umożliwiający pracę w domenie;
 |
| Oprogramowanie użytkowe | System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance + musi umożliwiać co najmniej:1. Wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,
2. Wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,
3. Stosowanie kwarantanny
4. Wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)
5. Skanowanie urządzeń USB natychmiast po podłączeniu,
6. Automatyczne odłączanie zainfekowanej końcówki od sieci,
7. Skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji.
8. Zarządzanie stacją kliencką poprzez zbieranie informacji co najmniej o: nazwie, 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 (procesor, RAM, SN, dysk), BIOS, interfejsach sieciowych, dołączonych peryferiach.
9. Musi posiadać moduł ochrony IDS/IPS
10. Musi posiadać mechanizm wykrywania skanowania portów
11. Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów
12. Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości
13. Oprogramowanie do szyfrowania, chroniące dane na stacji za pomocą algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH.
14. Pełne szyfrowanie dysków działających w oferowanych komputerach zapobiegające utracie danych z powodu utraty / kradzieży stacji roboczej.
15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak pendrive, dyski USB i udostępniać ją tylko autoryzowanym użytkownikom.
16. Musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji;
17. Musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji.
18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB oraz możliwości uruchamiania oprogramowania z takich dysków. Blokada ta musi umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.
19. Interfejs zarządzania musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji.
20. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware poprzez ograniczenie możliwości modyfikowania chronionych plików, tylko do procesów systemowych oraz zaufanych aplikacji.
21. Możliwość zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika.
22. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych ochroną any ransomware.
23. Monitorowanie krytycznych danych użytkownika zapobiegające atakom ransomware;
24. Centralna konsola zarządzająca umożliwiająca co najmniej:
25. przechowywanie danych w bazie typu SQL
26. zdalną instalację lub deinstalację oprogramowania, na pojedynczych stacjach, zakresie adresów IP lub grupie z ActiveDirectory;
27. tworzenie paczek instalacyjnych oprogramowania, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi oraz formatach dla systemów Linux
28. centralną dystrybucję uaktualnień definicji ochronnych, których źródłem będzie plik na serwerze konsoli;
29. raportowanie z prezentacją tabelaryczną i graficzną, możliwością automatycznego czyszczenia starych raportów, eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich;
30. definiowanie struktury opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji;
31. Możliwość tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera;
32. Dostęp do konsoli z dowolnego miejsca w nagłych przypadkach;
33. Możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń
34. 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.
35. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych;
36. System musi umożliwiać, z konsoli na serwerze, co najmniej:
37. różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie
38. przyznawanie praw dostępu dla nośników pamięci tj. USB, CD
39. regulowania połączeń WiFi i Bluetooth
40. kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe
41. blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi
42. blokowanie dostępu dowolnemu urządzeniu
43. tymczasowe dodanie dostępu do urządzenia przez administratora
44. szyfrowanie zawartości USB i udostępnianie jej na stacjach końcowych;
45. zablokowanie funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka
46. zezwalać na dostęp tylko urządzeniom wcześniej dodanym przez administratora
47. używania tylko zaufanych urządzeń sieciowych;
48. Funkcja wirtualnej klawiatury
49. Możliwość blokowania każdej aplikacji , w tym w oparciu o kategorie
50. Możliwość dodania własnych aplikacji do listy zablokowanych
51. Tworzenie listy aplikacji zainstalowanych na komputerach klientach poprzez konsolę administracyjną na serwerze
52. Kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool
53. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki;
54. Możliwość zablokowania funkcji Printscreen
55. Monitorowanie przesyłu danych między aplikacjami;
56. Monitorowanie i kontrola przepływu poufnych informacji
57. Blokowanie plików w oparciu o ich rozszerzenie lub rodzaj
58. Monitorowanie i zarządzanie danymi udostępnianymi poprzez zasoby sieciowe;
59. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe
60. Ochrona zawartości schowka systemu
61. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL
62. Dodawanie wyjątków dla domen, aplikacji i lokalizacji sieciowych
63. Ochrona plików zamkniętych w archiwach
64. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem
65. Możliwość tworzenia profilu DLP dla każdej polityki
66. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania
67. Ochrona przez wyciekiem plików poprzez programy typu p2p
68. Monitorowanie działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.
69. Monitorowanie określonych rodzajów plików.
70. Możliwość wykluczenia określonych plików/folderów z procedury monitorowania.
71. Możliwość śledzenia zmian we wszystkich plikach
72. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na stacjach roboczych;
73. Możliwość definiowana własnych typów plików
74. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku
75. Optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem
76. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich
77. System ochrony i zarządzania urządzeniami za pomocą platformy w chmurze;.
78. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi
79. Musi posiadać możliwość eksportu danych użytkownika
80. Import listy urządzeń z pliku CSV
81. Dodawanie urządzeń;
82. Podgląd co najmniej następujących informacji konfiguracji: data i status wdrożenia, status urządzenia, numer telefonu, właściciel, grupa, reguły, wersja agenta
83. Podgląd co najmniej następujących informacji sprzętowych: model, producent, system, adres MAC, bluetooth, wolna przestrzeń na dysku, całkowita przeszłość na dysku, użycie procesora,;
84. Podgląd zainstalowanych aplikacji;
85. Moduł raportowania aktywności, skanowania oraz naruszenia reguł;
86. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa dostępne przez przeglądarkę internetową;
87. Portal zarządzający w postaci SaaS;
88. Skanowanie podatności za pomocą nodów skanujących;
89. Nody skanujące w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie
90. Portal zarządzający musi umożliwiać:
91. przegląd wybranych danych;
92. zablokowanie możliwości zmiany konfiguracji;
93. zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów;
94. tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności
95. eksport skanów podatności do pliku CSV;
96. Deduplikacja danych na źródle,
97. Backup przyrostowy i różnicowy,
98. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,
99. Backup danych lokalnych – plikowy oraz poczty;
100. Backup otwartych plików;
101. Filtr plików oraz folderów,
102. Domyślne wykluczenia zbędnych plików;
103. Wyłączanie komputera po wykonaniu backup;
104. Przywracanie danych do wskazanej lokalizacji,
105. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,
106. Wyszukiwanie plików w repozytorium użytkownika,
107. Automatyczne logowanie,
108. Zapamiętywanie danych logowania,
109. Automatyczne uruchamianie programu przy starcie systemu,
110. Ustawianie priorytetu dla procesu backupu,
111. Zmiana klucza szyfrującego,
112. Ustawienia przepustowości/zajętości pasma,
113. Konfiguracja wydajności procesu backupu,
114. Zastępowanie nazwy pliku GUID-em,
115. Szyfrowanie danych algorytmem AES 256 CBC;
116. Kompresja danych,
117. Deklaracja klucza szyfrującego dane użytkownika,
118. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,
119. Obliczanie sumy kontrolnej,
120. Licencje z przestrzenią w chmurze –50 GB.
121. Wsparcie techniczne, świadczone przez producenta, w języku polskim;
122. **U**pgrade i instalację wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,
123. Sprawdzenie przed instalacją każdego sterownika, aplikacji, BIOS’u bezpośrednio na stronie producenta, a w szczególności uzyskanie informacji o:
	* poprawkach i usprawnieniach dotyczących aktualizacji
	* dacie wydania aktualizacji
	* priorytecie aktualizacji
	* zgodności z systemem operacyjnym
	* jakiego komponentu sprzętu dotyczy aktualizacja
	* wszystkich poprzednich aktualizacjach z informacjami jak powyżej;
124. Uzyskanie listy najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne
125. Włączenie/wyłączenie funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika lub aplikacji;
126. Rozpoznanie modelu oferowanego komputera, numeru seryjnego, informację kiedy dokonany został ostatnio upgrade;
127. Sprawdzenia historii upgradeów z informacją jakie sterowniki były instalowane z dokładną datą i wersją;
128. Wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji;
129. Wygenerowanie raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją jakich komponentów dotyczyły oraz błędach podczas instalowania. Raport musi zawierać z datą ( dd-mm-rrrr ) i godzinę podjętych i wykonanych akcji w okresie co najmniej roku wstecz.
 |

1. **Oprogramowanie biurowe – 25 szt.**

Kompletny pakiet oprogramowania biurowego musi spełniać następujące wymagania, poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Wymagania odnośnie interfejsu użytkownika:

1. Pełna polska wersja językowa interfejsu użytkownika;
2. Prostota i intuicyjność obsługi, pozwalająca na prace osobom

nieposiadającym umiejętności technicznych;

1. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej musi być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się;
2. Oprogramowanie musi umożliwiać tworzenie i edycje dokumentów elektronicznych w formacie, który spełnia następujące warunki:
3. posiada kompletny i publicznie dostępny opis formatu,
4. ma zdefiniowany układ informacji w postaci XML zgodnie z Tabela B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
5. umożliwia wykorzystanie schematów XML
6. wspiera w swojej specyfikacji podpis elektroniczny zgodnie z Tabela A.1.1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766)
7. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb użytkownika oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców;
8. W skład oprogramowania muszą wchodzić narzędzia umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami;
9. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim;.
10. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
11. Edytor tekstów
12. Arkusz kalkulacyjny
13. Narzędzie do przygotowywania i prowadzenia prezentacji/ tworzenia, edytowania i wyświetlania prezentacji
14. Narzędzie do zarzadzania informacja prywatną (poczta elektroniczna, kalendarzem, kontaktami i zadaniami)
15. Edytor tekstu musi umożliwiać:
16. Edycję i formatowanie tekstu w języku polskim wraz z obsługa języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
17. Wstawianie oraz formatowanie tabel
18. Wstawianie oraz formatowanie obiektów graficznych
19. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne)
20. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków
21. Automatyczne tworzenie spisów treści
22. Formatowanie nagłówków i stopek stron
23. Sprawdzanie pisowni w języku polskim
24. Śledzenie zmian wprowadzonych przez użytkowników
25. Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności
26. Określenie układu strony (pionowa/pozioma)
27. Wydruk dokumentów
28. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarzadzania informacją prywatną
29. Prace na posiadanych przez zamawiającego dokumentach utworzonych przy pomocy Microsoft Word 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu
30. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
31. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostepniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem.
32. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
33. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostepniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.
34. Arkusz kalkulacyjny musi umożliwiać:
35. Tworzenie raportów tabelarycznych
36. Tworzenie wykresów liniowych (wraz linia trendu), słupkowych, kołowych
37. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
38. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
39. Obsługę kostek OLAP oraz tworzenie i edycje kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiazywanie problemów optymalizacyjnych
40. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczna zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
41. Wyszukiwanie i zamianę danych
42. Wykonywanie analiz danych przy użyciu formatowania warunkowego
43. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
44. Nagrywanie, tworzenie i edycje makr automatyzujących wykonywanie czynności
45. Formatowanie czasu, daty i wartości finansowych z polskim formatem
46. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
47. Zachowanie pełnej zgodności z formatami posiadanych przez zamawiającego plików utworzonych za pomocą oprogramowania Microsoft Excel 2010, 2013 i 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń..
48. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
49. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać przygotowywanie prezentacji multimedialnych oraz:
50. Prezentowanie przy użyciu projektora multimedialnego
51. Drukowanie w formacie umożliwiającym robienie notatek
52. Zapisanie w postaci tylko do odczytu.
53. Nagrywanie narracji dołączanej do prezentacji
54. Opatrywanie slajdów notatkami dla prezentera
55. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
56. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
57. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
58. Tworzenie animacji obiektów i całych slajdów
59. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
60. Pełna zgodność z formatami plików posiadanych przez zamawiającego, utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013 i 2016.
61. Narzędzie do zarzadzania informacja prywatna (poczta elektroniczna, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
62. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego
63. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców
64. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną
65. Automatyczne grupowanie poczty o tym samym tytule
66. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczna do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy
67. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia
68. Zarzadzanie kalendarzem
69. Udostępnianie kalendarza innym użytkownikom
70. Przeglądanie kalendarza innych użytkowników
71. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach
72. Zarzadzanie lista zadań
73. Zlecanie zadań innym użytkownikom
74. Zarzadzanie listą kontaktów
75. Udostępnianie listy kontaktów innym użytkownikom
76. Przeglądanie listy kontaktów innych użytkowników
77. Możliwość przesyłania kontaktów innym użytkowników
78. Licencja niewygasająca. Nie dopuszcza się licencji w modelu subskrypcyjnym;

**Zamawiający zastrzega sobie możliwość wezwania oferentów, którzy złożyli oferty niepodlegające odrzuceniu w niniejszym postępowaniu, do okazania zaoferowanego sprzętu i oprogramowania, w celu sprawdzenia ich zgodności z wymaganiami określonymi przez Zamawiającego w SIWZ.**

**Okazanie nastąpi w dniu wyznaczonym przez Zamawiającego, po terminie składania ofert. Zamawiający poinformuje o terminie przeprowadzenia okazania z co najmniej pięciodniowym wyprzedzeniem (dni kalendarzowe).**

**Niestawienie się oferenta w wyznaczonym czasie i miejscu na okazaniu (prezentacji) sprzętu i/lub oprogramowania, uznane będzie jako negatywny wynik okazania, tj. niepotwierdzenie przez oferenta wymagań określonych przez Zamawiającego, co będzie skutkowało odrzuceniem oferty na podstawie art. 226 ust. 1 pkt. 5 Ustawy Pzp.**