Załącznik nr 7

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętu komputerowego wraz z wyposażeniem i oprogramowaniem na potrzeby pracowni informatycznych, w ramach projektu pn.: „Młodzi Kościuszkowcy kreują jutro" - współfinansowanego ze środków Europejskiego Funduszu Społecznego Plus w ramach Programu Regionalnego Fundusze Europejskie dla Łódzkiego 2021-2027. Projekt nr FELD.08.07-IZ.00-0211/25-00.

Część 1 – sprzęt komputerowy

Lp.	Nazwa	Wymagane parametry techniczne	Ilość	Jednostka miary
1.	monitor interaktywny	Przekątna min. cale 86' Rozdzielczość monitora min.: 3840 x 2160 Jasność min.: 450 cd/m2 Kontrast min. 5000:1 Ilość wyświetlanych kolorów: 1073 mln Głośniki: Zintegrowane min.2x 20W Kąt widzenia poziom/pion min. : 178/178 Typ złączy min.: Wejścia tył: HDMI 2.0 x2, DisplayPort x1, USB-B x3, USB-C x1, USB-A x3, RS232 x1, RJ45 x1 Wejścia przód: USB-C x1, USB-B x1, HDMI x1, Jack x1 Wyjścia tył: RJ45 x1, HDMI x1, Audio x1, USB-C x1 Gwarancja: 36 miesięcy Wbudowany system operacyjny: Android Procesor min. : 4 rdzenie Pamięć RAM min.: 8 GB Pamięć wewnętrzna min.: 128 GB Sieć : Ethernet, Wi-Fi 6, Bluetooth 5.2 Punkty dotyku min.: 40 Certyfikat EDLA Android 14"	2	szt.
2.	zewnętrzna nagrywarka DVD/CD	"Interfejs USB 2.0 (Type-A), zasilanie z USB. Obsługiwane nośniki: CD-R/RW, CD-ROM, DVD±R, DVD±RW, DVD±R DL, DVD-ROM, M-DISC. Prędkość zapisu min.: CD-R/RW: min. 24× DVD±R: min. 8× DVD±RW: min. 6× DVD±R DL: min. 6× Prędkość odczytu: CD-R 24×, CD-RW 24×; DVD+R 8×, DVD-R 8×, DVD+RW 8×, DVD-RW 6×, DVD+R DL 6×, DVD-R DL 6×; M-DISC (DVD+R SL) 4×.	44	szt.

		Kompatybilność: Windows 8/10/11, macOS 10.6+. waga ≤ 400 g. W zestawie: kabel USB oraz oprogramowanie do nagrywania."		
3.	klawiatura	• Klawiatura pełnowymiarowa, przewodowa, przeznaczona dla graczy. Klawiatura podświetlana, materiał pod klawiaturą wchłaniający wilgoć i ciecz. • Klawiatura w układzie US-QWERTY z klawiaturą numeryczną. • 11 klawiszy multimedialnych. • Funkcja anti-ghosting dla 19 klawiszy. N-Key Rollover. • Minimum 7 kolorów podświetlenia oraz tryby dynamiczne Długość przewodu: min. 1,6 m	44	szt.
4.	mysz komputerowa	• Mysz optyczna o rozdzielczości Predefiniowane poziomy DPI min.(1200/2400/3500/5500/8000) Minimalna ilość kliknięć • 5 mln Sensor równoważny do Instant A825	44	szt.
5.	komputer stacjonarny dla nauczyciela	• Komputer stacjonarny. • Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu, poczty elektronicznej oraz sztucznej ineligencji AI. • Procesor, osiągający w teście PassMark CPU Mark wynik min. 30000 punktów według wyników ze strony https://www.cpubenchmark.net lub https://www.passmark.com – załączyć do oferty; • Procyon Office Productivity – co najmniej 5800 punktów	2	szt.

		• Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów, Oferent może zostać wezwany do dostarczenia Zamawiającemu oprogramowania testującego, komputera do testu oraz dokładnego opisu metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 5 dni od otrzymania zawiadomienia od Zamawiającego. • 32GB DDR5 5600 MHz, możliwość rozbudowy do 64GB. • Obsługa pamięci • 7000(O.C.) / 6800(O.C.) / 6600(O.C.) / 6400(O.C.) / 6200(O.C.) / 6000(O.C.) / 5800(O.C.) /5600 • 1TB SSD M.2 PCIe® 4.0x4 NVMe® • Płyta ze wsparciem dla dysków M.2 NVMe 22110, M.2 2280. • Złącza: • 2xDisplayPort • 1xHDMI • Karta graficzna z 12 GB VRAM, PCI Express 4.0 x16, osiągająca w teście PassMark 3D Graphics Mark wynik min. 30000 punktów według wyników ze strony https://www.videocardbenchmark.net lub https://www.passmark.com – załączyć do oferty; • Wsparcie dla sztucznej inteligencji AI TOP, DLSS 3 • Test wydajności AI Geekbench ML 21000 punktów, Benchmark UL Procyon: UL Procyon AI Computer Vision (float32) 1300 punktów.		

		• Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów, Oferent może zostać wezwany do dostarczenia Zamawiającemu oprogramowania testującego, komputera do testu oraz dokładnego opisu metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 5 dni od otrzymania zawiadomienia od Zamawiającego. • Wyposażona w dedykowany chipset dla oferowanego procesora. Wyposażona w interfejs SATA III (6 Gb/s) do obsługi dysków twardych. • Posiadająca 4 gniazda DDR5 UDIMM • Płyta główna i konstrukcja wspierająca konfiguracje dwu dyskową SSD M.2+ HDD 2,5''. • 1 x PCIe® 4.0 x16 • 1 x PCIe® 3.0 x4 • Tylne porty min.: • 1x USB-C® 3.2 Gen 2 (ze wsparciem transferu danych Thunderbolt) • 2x USB 3.2 Gen 1 • 4x USB 2.0 • 1x Ethernet (RJ-45) • 1x złącze zasilania • 3x audio connector (3.5mm) • Karta dźwiękowa zintegrowana z płytą główną; High Definition (HD) Audio • Obudowa o sumie wymiarów maksymalnie 105 cm. • Możliwość montażu pełnowymiarowych kart graficznych;		

		• Montaż beznarzędziowy dysków, napędu optycznego i kart rozszerzeń. • Możliwość montażu dysku 1x2,5"" oraz 2x 3,5"" wewnątrz obudowy • Wyposażona w 2x USB 3.2 Gen 1 oraz złącza mikrofonu i słuchawek z przodu obudowy. • Możliwość otwierania bez użycia narzędzi (wkręty ręczne) • Wyposażona w złącze Kensington Lock i ucho na kłódkę • Zasilacz o mocy 500W 80+ Bronze. • Komputer musi być wyprodukowany zgodnie z następującymi normami: ISO 9001, ISO 27001, ISO 28000 – załączyć do oferty certyfikaty; • Certyfikat ISO 14001 zarządzania środowiskiem. • Certyfikat EPEAT dla Polski lub innego państwa członkowskiego Unii Europejskiej lub • równoważny certyfikat wydany przez akredytowaną instytucję w analogicznym zakresie; • Deklarację zgodności UE i oznakowanie CE; • Certyfikat TCO. • BIOS zgodny ze specyfikacją UEFI • Możliwość obsługi klawiaturą oraz myszą • Możliwość, bez uruchamiania systemu operacyjnego, odczytania • wersji BIOS,; • Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego		

		• Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń • BIOS musi być w pełni obsługiwany przez interfejs myszy i klawiatury; • "System operacyjny 64 bitowy 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, • b) 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 języku 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 poziomów: menu, otwartego okna systemu operacyjnego;		

		• 7. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, • 8. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. • 9. Graficzne środowisko instalacji i konfiguracji w języku polskim • 10. Wbudowany system pomocy w języku polskim. • 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). • 12. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. • 13. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. • 14. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. • 15. Zabezpieczony hasłem hierarchiczny dostęp do systemu; • 16. Konta i profile użytkowników zarządzane zdalnie; • 17. Praca systemu w trybie ochrony kont użytkowników. • 18. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; • 19. Molliwość zablokowania urządzenia w ramach danego konta		

		tylko do uruchamiania wybranej aplikacji - tryb ""kiosk"". • 20. 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 • 21. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. • 22. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. • 23. Oprogramowanie dla tworzenia kopii zapasowych (Backup); • 24. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. • 25. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. • 26. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. • 27. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu); • 28. Wbudowany mechanizm wirtualizacji typu hypervisor;		

		• 29. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. • 30. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego. • 31. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; • 32. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. • 33. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; • 34. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików; • 35. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. • 36. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. • 37. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; • 38. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM • 39. Możliwość tworzenia i przechowywania kopii zapasowych		

		kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; • 40. Możliwość tworzenia wirtualnych kart inteligentnych. • 41. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) • 42. Wsparcie dla IPSEC oparte na politykach; • 43. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; • 44. Mechanizmy logowania w oparciu o: • a) Login i hasło, • b) Karty inteligentne i certyfikaty (smartcard), • c) Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM; • 45. Umożliwiający pracę w domenie; • System chroniący przed zagrożeniami, silnik 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 stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. • 8. 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. • 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 rezydujące na punktach końcowych za pomocą		

		silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. • 14. Zapobieganie utracie danych z powodu utraty / kradzieży laptopa; • 15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnića je tylko autoryzowanym użytkownikom. • 16. Oprogramowanie musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do laptopa; • 17. Oprogramowanie musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do laptopa; • 18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB; • 19. Blokada możliwości uruchamiania oprogramowania z takich dysków. • 20. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. • 21. Interfejs musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. • 22. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. • 23. Ograniczanie możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. • 24. Możliwość dowolnego zdefiniowania chronionych folderów		

		zawierających wrażliwe dane użytkownika. • 25. Aplikacje uruchamiane z zaufanych folderów musza mieć możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. • 26. Monitorowanie krytycznych danych użytkownika zapobiegające przed atakami ransomware; • 27. Konsola zarządzająca musi umożliwiać co najmniej: • a) przechowywanie danych w bazie typu SQL; • b) zdalną instalację lub deinstalację oprogramowania na laptopach, zakresie adresów IP lub grupie z ActiveDirectory; • c) tworzenie paczek instalacyjnych oprogramowaniaw formie plików .exe lub .msi; • d) centralna dystrybucja na zarządzanych laptopach uaktualnień definicji ochronnych bez dostępu do sieci Internet. • e) raportowanie, 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 konsoli, jak i danych/raportów zbieranych ze laptopach, w tym raporty o oprogramowaniu zainstalowanym na laptopach; • f) definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji; • 28. Program musi wyświetlać status bezpieczeństwa urządzeń końcowych		

		• zainstalowanych w różnych lokalizacjach; • 29. Musi umożliwiać tworzenie kopii zapasowych i przywracania plików konfiguracyjnych z serwera w chmurze; • 30. Musi umożliwić dostęp do chmury zgodnie z przypisaniem do grupy; • 31. Musi posiadać dostęp do konsoli z dowolnego miejsca; • 32. Musi umożliwiać przeglądanie raportów sumarycznych dla wszystkich urządzeń • 33. Musi umożliwiać raportowanie i powiadamianie za pomocą poczty elektronicznej • 34. Konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, zarządzania informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danyc; • 35. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych; • 36. Konsola systemu musi umożliwiać, co najmniej: • a) różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie • b) przyznanie praw dostępu dla nośników pamięci tj. USB, CD • c) regulowanie połączeń WiFi i Bluetooth • d) kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe		

		• e) blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi • f) blokowanie dostępu dowolnemu urządzeniu • g) tymczasowe dodania dostępu do urządzenia przez administratora • h) szyfrowanie zawartości urządzenia USB i udostępnianie go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu; • i) zablokowanie funkcjonalności portów USB dla urządzeń innych niż klawiatura i myszka • j) zezwalanie na dostęp tylko urządzeniom wcześniej dodanym przez administratora • k) używanie tylko zaufanych urządzeń sieciowych; • 37. Wirtualna klawiatury • 38. Możliwość blokowania każdej aplikacji • 39. Możliwość zablokowania aplikacji w oparciu o kategorie • 40. Możliwość dodania własnych aplikacji do listy zablokowanych • 41. Dodawanie aplikacji w formie portable • 42. Możliwość wyboru pojedynczej aplikacji w konkretnej wersji • 43. Wymagane kategorie aplikacji: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool • 44. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych,		

		takich jak wymienne urządzenia, udziały sieciowe czy schowki. • 45. Możliwość zablokowania funkcji Printscreen • 46. Monitorowania przesyłu danych między aplikacjami; • 47. Możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików • 48. Możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj • 49. Możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe • 50. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe • 51. Ochrona zawartości schowka systemu • 52. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL • 53. Możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych • 54. Ochrona plików zamkniętych w archiwach. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem • 55. Możliwość tworzenia profilu DLP dla każdej polityki • 56. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania • 57. Ochrona przez wyciekiem plików poprzez programy typu p2p • 58. Możliwość monitorowania działań związanych z obsługą plików, takich		

		jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. • 59. Monitorowanie określonych rodzajów plików. • 60. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. • 61. Możliwość śledzenia zmian we wszystkich plikach • 62. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na laptopach; • 63. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacja dysku • 64. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich • 65. Zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email • 66. Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, nazwisko, adres email, , numer telefonu, typ użytkownika • 67. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi • 68. Musi posiadać możliwość eksportu danych użytkownika • 69. Musi umożliwiać import listy urządzeń z pliku CSV • 70. Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych • 71. Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: data uruchomienia, status urządzenia, numer telefonu,		

		właściciel, typ właściciela, nazwa grupy, geolokacja, wersja agenta; • 72. Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, ID, adres MAC, bluetooth, sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora; • 73. Musi zawierać podgląd aktualnie zainstalowanych aplikacji • 74. Musi udostepniać informacje o zużyciu danych, a w tym: ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, • 75. Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł • 76. Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres • 77. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa: • 78. Dostęp za pomocą portalu dostępnego przez przeglądarkę internetową • 79. Portal musi być dostępny w postaci usługi hostowanej; • 80. Skanowanie podatności za pomocą nodów skanujących • 81. Nod skanujący musi być dostępny w postaci usługi hostowanej oraz w postaci aplikacji instalowanej lokalnie • 82. Portal zarządzający musi umożliwiać:		

		• a) przegląd wybranych danych na podstawie konfigurowalnych widgetów • b) zablokowanie możliwości zmiany widgetów • c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. • d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności • eksport wszystkich skanów podatności do pliku CSV		
6.	komputer dla ucznia	• Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu, poczty elektronicznej oraz sztucznej ineligencji AI. • Procesor, osiągający w teście PassMark CPU Mark wynik min. 25000 punktów według wyników ze strony https://www.cpubenchmark.net lub https://www.passmark.com – załączyć do oferty; • Procyon Office Productivity – co najmniej 5700 punktów • Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów, Oferent może zostać wezwany do dostarczenia Zamawiającemu oprogramowania testującego, komputera do testu oraz dokładnego opisu metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 5 dni od	24	szt.

		otrzymania zawiadomienia od Zamawiającego. • 32GB DDR5 5600 MHz, możliwość rozbudowy do 64GB. • Obsługa pamięci • 7000(O.C.) / 6800(O.C.) / 6600(O.C.) / 6400(O.C.) / 6200(O.C.) / 6000(O.C.) / 5800(O.C.) /5600 • 1TB SSD M.2 PCIe® 4.0x4 NVMe® • Płyta ze wsparciem dla dysków M.2 NVMe 22110. • Złącza: • 2xDisplayPort • 1xHDMI • Karta graficzna z 12 GB VRAM, PCI Express 4.0 x16, osiągająca w teście PassMark 3D Graphics Mark wynik 30000 punktów według wyników ze strony https://www.videocardbenchmark.net lub https://www.passmark.com – załączyć do oferty; • Wsparcie dla sztucznej inteligencji AI TOP. • Test wydajności AI Geekbench ML (ONNX CPU i DirectML) 22000 punktów, Benchmark UL Procyon: UL Procyon AI Computer Vision (float32) 1300 punktów. • Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów, Oferent może zostać wezwany do dostarczenia Zamawiającemu oprogramowania testującego, komputera do testu oraz dokładnego opisu metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w		

		terminie nie dłuższym niż 5 dni od otrzymania zawiadomienia od Zamawiającego. • Wyposażona w dedykowany chipset dla oferowanego procesora. Wyposażona w interfejs SATA III (6 Gb/s) do obsługi dysków twardych. • Posiadająca 4 gniazda DDR5 UDIMM • Płyta główna i konstrukcja wspierająca konfiguracje dwu dyskową SSD M.2+ HDD 2,5''. • 1 x PCIe® 4.0 x16 • 1 x PCIe® 3.0 x4 • Tylne porty: • 1x USB-C® 3.2 Gen 2 (ze wsparciem transferu danych Thunderbolt) • 2x USB 3.2 Gen 1 • 4x USB 2.0 • 1x Ethernet (RJ-45) • 1x złącze zasilania • 3x audio connector (3.5mm) • Karta dźwiękowa zintegrowana z płytą główną; High Definition (HD) Audio • Obudowa o sumie wymiarów maksymalnie 105 cm. • Możliwość montażu pełnowymiarowych kart graficznych; • Montaż beznarzędziowy dysków, napędu optycznego i kart rozszerzeń. • Możliwość montażu dysku 1x2,5"" oraz 2x 3,5"" wewnątrz obudowy • Wyposażona w 2x USB 3.2 Gen 1 oraz złącza mikrofonu i słuchawek z przodu obudowy. • Możliwość otwierania bez użycia narzędzi (wkręty ręczne)		

		• Wyposażona w złącze Kensington Lock i ucho na kłódkę • Zasilacz o mocy 500W 80+ Bronze. • Komputer musi być wyprodukowany zgodnie z następującymi normami: ISO 9001, ISO 27001, ISO 28000 – załączyć do oferty certyfikaty; • Certyfikat ISO 14001 zarządzania środowiskiem. • Certyfikat EPEAT dla Polski lub innego państwa członkowskiego Unii Europejskiej lub • równoważny certyfikat wydany przez akredytowaną instytucję w analogicznym zakresie; • Deklarację zgodności UE i oznakowanie CE; • Certyfikat TCO. • BIOS zgodny ze specyfikacją UEFI • Możliwość obsługi klawiaturą oraz myszą • Możliwość, bez uruchamiania systemu operacyjnego, odczytania • wersji BIOS,; • Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego • Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń • BIOS musi być w pełni obsługiwany przez interfejs myszy i klawiatury; • "System operacyjny 64 bitowy 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, • b) 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 języku 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 poziomów: menu, otwartego okna systemu operacyjnego; • 7. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, • 8. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. • 9. Graficzne środowisko instalacji i konfiguracji w języku polskim		

		• 10. Wbudowany system pomocy w języku polskim. • 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). • 12. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. • 13. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. • 14. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. • 15. Zabezpieczony hasłem hierarchiczny dostęp do systemu; • 16. Konta i profile użytkowników zarządzane zdalnie; • 17. Praca systemu w trybie ochrony kont użytkowników. • 18. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; • 19. Molliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb ""kiosk"". • 20. 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		

		• 21. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. • 22. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. • 23. Oprogramowanie dla tworzenia kopii zapasowych (Backup); • 24. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. • 25. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. • 26. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. • 27. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu); • 28. Wbudowany mechanizm wirtualizacji typu hypervisor; • 29. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. • 30. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego.		

		• 31. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; • 32. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. • 33. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; • 34. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików; • 35. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. • 36. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. • 37. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; • 38. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM • 39. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; • 40. Możliwość tworzenia wirtualnych kart inteligentnych. • 41. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)		

		• 42. Wsparcie dla IPSEC oparte na politykach; • 43. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; • 44. Mechanizmy logowania w oparciu o: • a) Login i hasło, • b) Karty inteligentne i certyfikaty (smartcard), • c) Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM; • 45. Umozliwiajacy pracę w domenie; • System chroniący przed zagrożeniami, silnik 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 stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. • 8. 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. • 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 rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. • 14. Zapobieganie utracie danych z powodu utraty / kradzieży laptopa; • 15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnića je tylko autoryzowanym użytkownikom.		

		• 16. Oprogramowanie musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do laptopa; • 17. Oprogramowanie musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do laptopa; • 18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB; • 19. Blokada możliwości uruchamiania oprogramowania z takich dysków. • 20. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. • 21. Interfejs musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. • 22. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. • 23. Ograniczanie możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. • 24. Możliwość dowolnego zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika. • 25. Aplikacje uruchamiane z zaufanych folderów musza mieć możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. • 26. Monitorowanie krytycznych danych użytkownika zapobiegające przed atakami ransomware;		

		• 27. Konsola zarządzająca musi umożliwiać co najmniej: • a) przechowywanie danych w bazie typu SQL; • b) zdalną instalację lub deinstalację oprogramowania na laptopach, zakresie adresów IP lub grupie z ActiveDirectory; • c) tworzenie paczek instalacyjnych oprogramowaniaw formie plików .exe lub .msi; • d) centralna dystrybucja na zarządzanych laptopach uaktualnień definicji ochronnych bez dostępu do sieci Internet. • e) raportowanie, 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 konsoli, jak i danych/raportów zbieranych ze laptopach, w tym raporty o oprogramowaniu zainstalowanym na laptopach; • f) definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji; • 28. Program musi wyświetlać status bezpieczeństwa urządzeń końcowych • zainstalowanych w różnych lokalizacjach; • 29. Musi umożliwiać tworzenie kopii zapasowych i przywracania plików konfiguracyjnych z serwera w chmurze; • 30. Musi umożliwić dostęp do chmury zgodnie z przypisaniem do grupy;		

		• 31. Musi posiadać dostęp do konsoli z dowolnego miejsca; • 32. Musi umożliwiać przeglądanie raportów sumarycznych dla wszystkich urządzeń • 33. Musi umożliwiać raportowanie i powiadamianie za pomocą poczty elektronicznej • 34. Konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, zarządzania informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danyc; • 35. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych; • 36. Konsola systemu musi umożliwiać, co najmniej: • a) różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie • b) przyznanie praw dostępu dla nośników pamięci tj. USB, CD • c) regulowanie połączeń WiFi i Bluetooth • d) kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe • e) blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi • f) blokowanie dostępu dowolnemu urządzeniu • g) tymczasowe dodania dostępu do urządzenia przez administratora • h) szyfrowanie zawartości urządzenia USB i udostępnianie go na punktach		

		końcowych z zainstalowanym oprogramowaniem klienckim systemu; • i) zablokowanie funkcjonalności portów USB dla urządzeń innych niż klawiatura i myszka • j) zezwalanie na dostęp tylko urządzeniom wcześniej dodanym przez administratora • k) używanie tylko zaufanych urządzeń sieciowych; • 37. Wirtualna klawiatury • 38. Możliwość blokowania każdej aplikacji • 39. Możliwość zablokowania aplikacji w oparciu o kategorie • 40. Możliwość dodania własnych aplikacji do listy zablokowanych • 41. Dodawanie aplikacji w formie portable • 42. Możliwość wyboru pojedynczej aplikacji w konkretnej wersji • 43. Wymagane kategorie aplikacji: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool • 44. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. • 45. Możliwość zablokowania funkcji Printscreen • 46. Monitorowania przesyłu danych między aplikacjami; • 47. Możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików		

		• 48. Możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj • 49. Możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe • 50. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe • 51. Ochrona zawartości schowka systemu • 52. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL • 53. Możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych • 54. Ochrona plików zamkniętych w archiwach. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem • 55. Możliwość tworzenia profilu DLP dla każdej polityki • 56. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania • 57. Ochrona przez wyciekiem plików poprzez programy typu p2p • 58. Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. • 59. Monitorowanie określonych rodzajów plików. • 60. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.		

		• 61. Możliwość śledzenia zmian we wszystkich plikach • 62. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na laptopach; • 63. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacja dysku • 64. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich • 65. Zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email • 66. Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, nazwisko, adres email, , numer telefonu, typ użytkownika • 67. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi • 68. Musi posiadać możliwość eksportu danych użytkownika • 69. Musi umożliwiać import listy urządzeń z pliku CSV • 70. Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych • 71. Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: data uruchomienia, status urządzenia, numer telefonu, właściciel, typ właściciela, nazwa grupy, geolokacja, wersja agenta; • 72. Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, ID, adres MAC, bluetooth, sieć, wolna przestrzeń na dysku,		

		całkowita przeszłość na dysku, bateria, zużycie procesora; • 73. Musi zawierać podgląd aktualnie zainstalowanych aplikacji • 74. Musi udostepniać informacje o zużyciu danych, a w tym: ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, • 75. Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł • 76. Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres • 77. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa: • 78. Dostęp za pomocą portalu dostępnego przez przeglądarkę internetową • 79. Portal musi być dostępny w postaci usługi hostowanej; • 80. Skanowanie podatności za pomocą nodów skanujących • 81. Nod skanujący musi być dostępny w postaci usługi hostowanej oraz w postaci aplikacji instalowanej lokalnie • 82. Portal zarządzający musi umożliwiać: • a) przegląd wybranych danych na podstawie konfigurowalnych widgetów • b) zablokowanie możliwości zmiany widgetów • c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.		

		• d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności • eksport wszystkich skanów podatności do pliku CSV		
7.	komputery dla uczniów	• "Komputer stacjonarny. • Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu, poczty elektronicznej oraz sztucznej ineligencji AI. • Procesor, osiągający w teście PassMark CPU Mark wynik min. 25000 punktów według wyników ze strony https://www.cpubenchmark.net lub https://www.passmark.com – załączyć do oferty; • Procyon Office Productivity – co najmniej 5700 punktów • Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów, Oferent może zostać wezwany do dostarczenia Zamawiającemu oprogramowania testującego, komputera do testu oraz dokładnego opisu metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 5 dni od otrzymania zawiadomienia od Zamawiającego. • 16GB DDR5 5600 MHz, możliwość rozbudowy do 64GB. • Obsługa pamięci • 7000(O.C.) / 6800(O.C.) / 6600(O.C.) / 6400(O.C.) / 6200(O.C.) / 6000(O.C.) / 5800(O.C.) /5600	18	szt.

		• 1TB SSD M.2 PCIe® 4.0x4 NVMe® • Złącza: • 2xDisplayPort • 1xHDMI • Karta graficzna z 8 GB VRAM, PCI Express 4.0 x16, osiągająca w teście PassMark 3D Graphics Mark wynik 19600 punktów według wyników ze strony https://www.videocardbenchmark.net lub https://www.passmark.com – załączyć do oferty; • Wsparcie dla sztucznej inteligencji AI TOP, DLSS 3 • Test wydajności UL Procyon AI Computer Vision (float16)) 1500 punktów, Benchmark UL Procyon: UL Procyon AI Computer Vision (float32) 800 punktów. • Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów, Oferent może zostać wezwany do dostarczenia Zamawiającemu oprogramowania testującego, komputera do testu oraz dokładnego opisu metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 5 dni od otrzymania zawiadomienia od Zamawiającego. • Wyposażona w dedykowany chipset dla oferowanego procesora. Wyposażona w interfejs SATA III (6 Gb/s) do obsługi dysków twardych. • Posiadająca 2 gniazda DDR5 UDIMM		

		• Płyta główna i konstrukcja wspierająca konfiguracje dwu dyskową SSD M.2+ HDD 2,5''. • 1xPCIe 4.0x16 • 1 x PCIe® 4.0 x4 • Tylne porty: • 2x USB 3.2 Gen 1 • 4x USB 2.0 • 1x Ethernet (RJ-45) • 1x złącze zasilania • 3x audio connector (3.5mm) • Karta dźwiękowa zintegrowana z płytą główną; High Definition (HD) Audio • Obudowa o sumie wymiarów maksymalnie 105 cm. • Możliwość montażu pełnowymiarowych kart graficznych; • Montaż beznarzędziowy dysków, napędu optycznego i kart rozszerzeń. • Możliwość montażu dysku 1x2,5"" oraz 1x 3,5"" wewnątrz obudowy • Wyposażona w 1x USB 3.2 Gen 1 1x USB Type-C oraz złącza mikrofonu i słuchawek z przodu obudowy. • Wyposażona w złącze Kensington Lock i ucho na kłódkę • Zasilacz o mocy 500W 80+ Bronze. • Komputer musi być wyprodukowany zgodnie z następującymi normami: ISO 9001, ISO 27001, ISO 28000 – załączyć do oferty certyfikaty; • Certyfikat ISO 14001 zarządzania środowiskiem. • Certyfikat EPEAT dla Polski lub innego państwa członkowskiego Unii Europejskiej lub		

		• równoważny certyfikat wydany przez akredytowaną instytucję w analogicznym zakresie; • Deklarację zgodności UE i oznakowanie CE; • Certyfikat TCO. • BIOS zgodny ze specyfikacją UEFI • Możliwość obsługi klawiaturą oraz myszą • Możliwość, bez uruchamiania systemu operacyjnego, odczytania • wersji BIOS,; • Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego • Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń • BIOS musi być w pełni obsługiwany przez interfejs myszy i klawiatury; • "System operacyjny 64 bitowy 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, • b) 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 języku 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 poziomów: menu, otwartego okna systemu operacyjnego; • 7. System wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, • 8. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. • 9. Graficzne środowisko instalacji i konfiguracji w języku polskim • 10. Wbudowany system pomocy w języku polskim. • 11. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). • 12. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora Zamawiającego. • 13. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.		

		• 14. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, w tym możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. • 15. Zabezpieczony hasłem hierarchiczny dostęp do systemu; • 16. Konta i profile użytkowników zarządzane zdalnie; • 17. Praca systemu w trybie ochrony kont użytkowników. • 18. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze; • 19. Molliwość zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb ""kiosk"". • 20. 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 • 21. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. • 22. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. • 23. Oprogramowanie dla tworzenia kopii zapasowych (Backup);		

		• 24. Automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. • 25. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. • 26. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. • 27. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu); • 28. Wbudowany mechanizm wirtualizacji typu hypervisor; • 29. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem interfejsu graficznego. • 30. Bezpłatne biuletyny bezpieczeństwa związane z działaniem systemu operacyjnego. • 31. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; • 32. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. • 33. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny; • 34. Zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej i udostępnianiem plików;		

		• 35. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. • 36. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi i niezarządzanymi. • 37. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne; • 38. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM • 39. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych; • 40. Możliwość tworzenia wirtualnych kart inteligentnych. • 41. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) • 42. Wsparcie dla IPSEC oparte na politykach; • 43. Wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; • 44. Mechanizmy logowania w oparciu o: • a) Login i hasło, • b) Karty inteligentne i certyfikaty (smartcard), • c) Wirtualne karty inteligentne i certyfikaty chronione poprzez moduł TPM;		

		• 45. Umozliwiajacy pracę w domenie; • System chroniący przed zagrożeniami, silnik 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 stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. • 8. 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. • 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 rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. • 14. Zapobieganie utracie danych z powodu utraty / kradzieży laptopa; • 15. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnića je tylko autoryzowanym użytkownikom. • 16. Oprogramowanie musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do laptopa; • 17. Oprogramowanie musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do laptopa; • 18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB; • 19. Blokada możliwości uruchamiania oprogramowania z takich dysków.		

		• 20. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. • 21. Interfejs musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. • 22. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. • 23. Ograniczanie możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. • 24. Możliwość dowolnego zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika. • 25. Aplikacje uruchamiane z zaufanych folderów musza mieć możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. • 26. Monitorowanie krytycznych danych użytkownika zapobiegające przed atakami ransomware; • 27. Konsola zarządzająca musi umożliwiać co najmniej: • a) przechowywanie danych w bazie typu SQL; • b) zdalną instalację lub deinstalację oprogramowania na laptopach, zakresie adresów IP lub grupie z ActiveDirectory; • c) tworzenie paczek instalacyjnych oprogramowaniaw formie plików .exe lub .msi; • d) centralna dystrybucja na zarządzanych laptopach uaktualnień		

		definicji ochronnych bez dostępu do sieci Internet. • e) raportowanie, 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 konsoli, jak i danych/raportów zbieranych ze laptopach, w tym raporty o oprogramowaniu zainstalowanym na laptopach; • f) definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji; • 28. Program musi wyświetlać status bezpieczeństwa urządzeń końcowych • zainstalowanych w różnych lokalizacjach; • 29. Musi umożliwiać tworzenie kopii zapasowych i przywracania plików konfiguracyjnych z serwera w chmurze; • 30. Musi umożliwić dostęp do chmury zgodnie z przypisaniem do grupy; • 31. Musi posiadać dostęp do konsoli z dowolnego miejsca; • 32. Musi umożliwiać przeglądanie raportów sumarycznych dla wszystkich urządzeń • 33. Musi umożliwiać raportowanie i powiadamianie za pomocą poczty elektronicznej • 34. Konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, zarządzania informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danyc;		

		• 35. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych; • 36. Konsola systemu musi umożliwiać, co najmniej: • a) różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie • b) przyznanie praw dostępu dla nośników pamięci tj. USB, CD • c) regulowanie połączeń WiFi i Bluetooth • d) kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe • e) blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi • f) blokowanie dostępu dowolnemu urządzeniu • g) tymczasowe dodania dostępu do urządzenia przez administratora • h) szyfrowanie zawartości urządzenia USB i udostępnianie go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu; • i) zablokowanie funkcjonalności portów USB dla urządzeń innych niż klawiatura i myszka • j) zezwalanie na dostęp tylko urządzeniom wcześniej dodanym przez administratora • k) używanie tylko zaufanych urządzeń sieciowych; • 37. Wirtualna klawiatury • 38. Możliwość blokowania każdej aplikacji		

		• 39. Możliwość zablokowania aplikacji w oparciu o kategorie • 40. Możliwość dodania własnych aplikacji do listy zablokowanych • 41. Dodawanie aplikacji w formie portable • 42. Możliwość wyboru pojedynczej aplikacji w konkretnej wersji • 43. Wymagane kategorie aplikacji: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool • 44. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. • 45. Możliwość zablokowania funkcji Printscreen • 46. Monitorowania przesyłu danych między aplikacjami; • 47. Możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików • 48. Możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj • 49. Możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe • 50. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe • 51. Ochrona zawartości schowka systemu • 52. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL		

		• 53. Możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych • 54. Ochrona plików zamkniętych w archiwach. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem • 55. Możliwość tworzenia profilu DLP dla każdej polityki • 56. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania • 57. Ochrona przez wyciekiem plików poprzez programy typu p2p • 58. Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. • 59. Monitorowanie określonych rodzajów plików. • 60. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. • 61. Możliwość śledzenia zmian we wszystkich plikach • 62. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na laptopach; • 63. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacja dysku • 64. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich • 65. Zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email		

		• 66. Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, nazwisko, adres email, , numer telefonu, typ użytkownika • 67. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi • 68. Musi posiadać możliwość eksportu danych użytkownika • 69. Musi umożliwiać import listy urządzeń z pliku CSV • 70. Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych • 71. Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: data uruchomienia, status urządzenia, numer telefonu, właściciel, typ właściciela, nazwa grupy, geolokacja, wersja agenta; • 72. Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, ID, adres MAC, bluetooth, sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora; • 73. Musi zawierać podgląd aktualnie zainstalowanych aplikacji • 74. Musi udostepniać informacje o zużyciu danych, a w tym: ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, • 75. Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł • 76. Moduł raportowania musi umożliwiać podgląd w zakresie:		

		dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres • 77. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa: • 78. Dostęp za pomocą portalu dostępnego przez przeglądarkę internetową • 79. Portal musi być dostępny w postaci usługi hostowanej; • 80. Skanowanie podatności za pomocą nodów skanujących • 81. Nod skanujący musi być dostępny w postaci usługi hostowanej oraz w postaci aplikacji instalowanej lokalnie • 82. Portal zarządzający musi umożliwiać: • a) przegląd wybranych danych na podstawie konfigurowalnych widgetów • b) zablokowanie możliwości zmiany widgetów • c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. • d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności • eksport wszystkich skanów podatności do pliku CSV		
8.	monitory dla uczniów	Minimalne parametry techniczne Przekątna ekranu27" Powłoka matrycy MatowaRodzaj matrycyLED, IPSTyp ekranuPłaskiMonitor bezramkowyTak Rozdzielczość2560×1440 (WQHD)Format obrazu16:9O dświeżaniemin. 165 HzKolorsRGB ≥ 99%, DCI-P3 ≥ 90% Liczba kolorów 1,07 mld HDRDisplayHDR 400 (lub kompatybilne) Czas reakcji≤ 1 ms MPRT	44	szt.

		SynchronizacjaFreeSync Premium / Adaptive SyncOchrona oczu Low Blue Light + Flicker-Free. Wielkość plamki ok. 0,233 mm Kontrast statyczny min. 1000:1 Jasność min. 350 cd/m² Kąty widzenia 178° / 178°Złączamin. 1× HDMI, min. 1× DisplayPort, audio-out Głośniki min. 2× 3W. Regulacja pivot, tilt, wysokość Gwarancja min. 2 lata		
9.	kamery internetowe z mikrofonem	• Kamera internetowa z mikrofonem • Typ sensora: CMOS • Materiał soczewki szkło • Rozdzielczość min.: 1920 x 1080 • Poprzeczny punkt widzenia min.(diagonalny) 78° • Rozdzielczość przy prędkości przechwytywania 1280x720@60fps, 1920x1080@30fps • Kompresja wideo: H.264 • Obsługiwane tryby wideo 720p, 1080p • Automatyczne ustawienie ostrości Tak • Funkcja aparatu cyfrowego: Tak • Typ mocowania Klips/Stojak • Interfejs: USB • Zasilanie: USB • Mikrofon wbudowany: Dwa mikrofony stereo / wielokierunkowe • Funkcja wideokonferencji: Tak • Automatyczna korekcja światła Tak • Wyposażenie: Kabel USB, Statyw	44	szt.
10.	drukarka ze skanerem	• Typ drukarkiKolorowa atramentowa, technologia PrecisionCore (lub równoważna). • Funkcje Drukowanie, kopiowanie, skanowanie, faksowanie (4w1).	2	szt.

		• Interfejs USB, Gigabit Ethernet, Wi-Fi 802.11b/g/n, Wi-Fi Direct. • Rozdzielczość kopiowania Co najmniej 600 × 600 dpi. • Szybkość kopiowania Zgodna z prędkością ISO: 25 str./min mono, 12 str./min kolor • Obsługiwane formaty A3+, A3, A4, A5, koperty, nośniki specjalne. • Szybkość drukowania dwustronnego A4 Duplex automatyczny realnie ok. 10–12 str./min. • Szybkość kopiowania A4jak wyżej – zgodna z ISO 25/12 ppm. • Szybkość druku w kolorze 12 str./min. • Szybkość druku w czerni 25 str./min • Rozdzielczość drukowania4800 × 2400 dpi. • Rozdzielczość kopiowania 600 × 600 dpi. • Rozdzielczość skanowania Optyczna 600 dpi. • Skanowanie z ADF do A3/A3+ (duplex). • Drukowanie z USBPDF, JPEG, TIFF (zgodne z Epson iPrint / USB host). • Rozdzielczość faksu minimum 200 × 200 dpi. • Kopiowanie – dwustronne • Automatyczne – duplex w ADF. • Podajniki papieru 2 × 250 arkuszy + tylny podajnik 50 arkuszy + odbiornik 100–125 arkuszy. • Poziom hałasu Do 60 dB. • Zużycie energii zwykle ≤50 W • Ekran LCDKolorowy ekran dotykowy 10,9 cm.		

		• Obciążenie miesięczne 50 000 stron, zalecane 200–2500 stron. • Łączność bezprzewodowa Wi-Fi 802.11b/g/n, Wi-Fi Direct, LAN. • WagaOkoło 20 kg Wymagania dodatkowe • Automatyczny dupleks druku oraz dupleks skanowania (ADF). • GwarancjaMinimum 2 lata."		
11.	listwa zasilajaca	• TypAntyprzepięciowa • Liczba gniazd sieciowych 8 szt. z uziemieniem; • Długość przewodu min. 3 m. • Czas reakcji układu przeciwprzepięciowego Maksymalnie 25 ns • Zabezpieczenie nadprądowe Bezpiecznik automatyczny 10 A, wbudowany warystor • Wymaganie dodatkowe Podświetlany wyłącznik sieciowy • Maksymalne obciążenie [W] 2300	24	Szt.

Część 2 – oprogramowanie

Lp.	Nazwa	Wymagane parametry techniczne	Ilość	Jednostka miary
1.	upgrade systemu operacyjnego	UPGRADE'u systemu operacyjnego: Windows 10 Home (DPK) x64 PL Windows 11 Home (DPK) x64 PL Do wersji Professional: Windows 10 Pro (DPK) x64 PL Windows 11 Pro (DPK) x64 PL	44	szt.
2.	program antywirusowy	Licencja na min. 100 PC. System chroniący przed zagrożeniami, silnik musi umożliwiać co najmniej: 1. Wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które	1	szt.

		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 stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. 8. 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. 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 rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. 14. Zapobieganie utracie danych z powodu utraty / kradzieży laptopa; 15. Oprogramowanie musi szyfrować całą		

		zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnića je tylko autoryzowanym użytkownikom. 16. Oprogramowanie musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do laptopa; 17. Oprogramowanie musi umożliwiać zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do laptopa; 18. Możliwość blokady zapisywania plików na zewnętrznych dyskach USB; 19. Blokada możliwości uruchamiania oprogramowania z takich dysków. 20. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. 21. Interfejs musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. 22. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. 23. Ograniczanie możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. 24. Możliwość dowolnego zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika. 25. Aplikacje uruchamiane z zaufanych folderów musza mieć możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. 26. Monitorowanie krytycznych danych użytkownika zapobiegające przed atakami ransomware; 27. Konsola zarządzająca musi umożliwiać co najmniej: a) przechowywanie danych w bazie typu SQL; b) zdalną instalację lub deinstalację oprogramowania na laptopach, zakresie adresów IP lub grupie z ActiveDirectory; c) tworzenie paczek instalacyjnych oprogramowaniaw formie plików .exe lub .msi; d) centralna dystrybucja na zarządzanych		

		laptopach uaktualnień definicji ochronnych bez dostępu do sieci Internet. e) raportowanie, 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 konsoli, jak i danych/raportów zbieranych ze laptopach, w tym raporty o oprogramowaniu zainstalowanym na laptopach; f) definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji; 28. Program musi wyświetlać status bezpieczeństwa urządzeń końcowych zainstalowanych w różnych lokalizacjach; 29. Musi umożliwiać tworzenie kopii zapasowych i przywracania plików konfiguracyjnych z serwera w chmurze; 30. Musi umożliwić dostęp do chmury zgodnie z przypisaniem do grupy; 31. Musi posiadać dostęp do konsoli z dowolnego miejsca; 32. Musi umożliwiać przeglądanie raportów sumarycznych dla wszystkich urządzeń 33. Musi umożliwiać raportowanie i powiadamianie za pomocą poczty elektronicznej 34. Konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, zarządzania informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danyc; 35. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych; 36. Konsola systemu musi umożliwiać, co najmniej: a) różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie b) przyznanie praw dostępu dla nośników pamięci tj. USB, CD c) regulowanie połączeń WiFi i Bluetooth d) kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe		

		e) blokadę lub zezwolenia na połączenie się z urządzeniami mobilnymi f) blokowanie dostępu dowolnemu urządzeniu g) tymczasowe dodania dostępu do urządzenia przez administratora h) szyfrowanie zawartości urządzenia USB i udostępnianie go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu; i) zablokowanie funkcjonalności portów USB dla urządzeń innych niż klawiatura i myszka j) zezwalanie na dostęp tylko urządzeniom wcześniej dodanym przez administratora k) używanie tylko zaufanych urządzeń sieciowych; 37. Wirtualna klawiatury 38. Możliwość blokowania każdej aplikacji 39. Możliwość zablokowania aplikacji w oparciu o kategorie 40. Możliwość dodania własnych aplikacji do listy zablokowanych 41. Dodawanie aplikacji w formie portable 42. Możliwość wyboru pojedynczej aplikacji w konkretnej wersji 43. Wymagane kategorie aplikacji: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool 44. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. 45. Możliwość zablokowania funkcji Printscreen 46. Monitorowania przesyłu danych między aplikacjami; 47. Możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików 48. Możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj 49. Możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe 50. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe		

		51. Ochrona zawartości schowka systemu 52. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL 53. Możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych 54. Ochrona plików zamkniętych w archiwach. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem 55. Możliwość tworzenia profilu DLP dla każdej polityki 56. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania 57. Ochrona przez wyciekiem plików poprzez programy typu p2p 58. Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. 59. Monitorowanie określonych rodzajów plików. 60. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. 61. Możliwość śledzenia zmian we wszystkich plikach 62. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na laptopach; 63. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacja dysku 64. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich 65. Zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email 66. Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, nazwisko, adres email, , numer telefonu, typ użytkownika 67. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi 68. Musi posiadać możliwość eksportu danych użytkownika 69. Musi umożliwiać import listy urządzeń z		

		pliku CSV 70. Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych 71. Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: data uruchomienia, status urządzenia, numer telefonu, właściciel, typ właściciela, nazwa grupy, geolokacja, wersja agenta; 72. Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, ID, adres MAC, bluetooth, sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora; 73. Musi zawierać podgląd aktualnie zainstalowanych aplikacji 74. Musi udostepniać informacje o zużyciu danych, a w tym: ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, 75. Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł 76. Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres 77. Oprogramowanie pozwalające na wykrywanie oraz zarządzanie podatnościami bezpieczeństwa: 78. Dostęp za pomocą portalu dostępnego przez przeglądarkę internetową 79. Portal musi być dostępny w postaci usługi hostowanej; 80. Skanowanie podatności za pomocą nodów skanujących 81. Nod skanujący musi być dostępny w postaci usługi hostowanej oraz w postaci aplikacji instalowanej lokalnie 82. Portal zarządzający musi umożliwiać: a) przegląd wybranych danych na podstawie konfigurowalnych widgetów b) zablokowanie możliwości zmiany widgetów c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.		

		d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności eksport wszystkich skanów podatności do pliku CSV		

UWAGA: W przypadku, gdy Zamawiający posługuje się w opisie przedmiotu zamówienia nazwami produktów dopuszcza się użycie przedmiotu równoważnego, który spełni standardy jakościowe, parametry techniczne, warunki docelowego przeznaczenia oraz funkcji i walorów użytkowych produktu wskazanego z nazwy. Nazwy handlowe produktów użyte w opisie przedmiotu zamówienia powinny być traktowanie jedynie jako definicje standardu jakiego wymaga Zamawiający.
Wykonawca określi cenę zakupu, dostawy w formularzu cenowym – załącznik nr 1 do zapytania ofertowego. Cena oferty musi uwzględniać wszystkie koszty niezbędne do realizacji zamówienia.
Cena może być tylko jedna za oferowany przedmiot zamówienia.
Oferowany sprzęt ma być fabrycznie nowy, nieużywany oraz nieeksponowany na wystawach lub imprezach targowych, sprawny technicznie, bezpieczny, kompletny i gotowy do pracy, a także musi spełniać wymagania techniczno-funkcjonalne wyszczególnione w opisie przedmiotu zamówienia.

Zbigniew Wiśniewski