Opis przedmiotu zamówienia część I - OPZ I

I. Stacja robocza – 12 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 z oprogramowania testującego 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.). Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego
Pamięć operacyjna RAM	32GB DDR4 3200 MHz non-ECC możliwość rozbudowy do min 128GB, cztery sloty na pamięć RAM.
Parametry pamieci masowej	500GB SSD PCIe Komputer musi umożliwiać instalację min 3 HDD, dopuszcza się konfigurację dysk M.2 + 2 dyski magnetyczne
Wydajność grafiki	Osiągająca w teście SysMark25 Creativity co najmniej 1300 punktów. **Wydruk z oprogramowania testującego załączyć do oferty.**
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 audio out. Czytnik kart multimedialnych czytający karty SD 4.0
Obudowa	Typu SFF z obsługą kart PCI Express wyłącznie o niskim profilu, wyposażona 1 wnękę 2,5” lub 3,5” wewnętrzne, 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 70 cm; Zasilacz o mocy 300W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności 90% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności

	min. 89% przy obciążeniu zasilacza na poziomie 100%, Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego, dysku 3,5" oraz 2,5" bez konieczności użycia narzędzi. Wyklucza się użycia wkrętów, śrub motylkowych, śrub radełkowych. Obudowa musi posiadać czujnik otwarcia współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki; Obudowa 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. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
Bezpieczeństwo	Układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu 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	Wbudowana w płytę główną technologia zarządzania i monitorowania komputera 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) 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/);
Wirtualizacja	Sprzętowe wsparcie technologi wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głowej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą myszy czyli swobodne poruszanie się po menu we/wy oraz wł/wy funkcji bez używania klawiatury; Informacje dostępne z poziomu BIOS na potrzeby inwentaryzacji: wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach, procesor (typ, nazwa, typowa prędkość, minimalna, maksymalna), pojemności zainstalowanych dysków twardych MAC adres zintegrowanej karty sieciowej, kontroler audio. Informacje dostępne w samym menu BIOS bez stosowania dodatkowego oprogramowania jak i wbudowanego systemu diagnostycznego. Możliwość, ustawienia hasła na poziomie administratora i użytkownika; 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, 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 w szczególności: pamięci, procesora, dysku.
Certyfikaty i standardy	Urządzenia muszą być wyprodukowane zgodnie z normami: ISO 9001 i ISO 50001 – **załączyć do oferty certyfikaty dla producenta sprzętu;** Certyfikat TCO, wymagana certyfikacja na stronie - http://tco.brightly.se/pls/nvp/!tco_search – **załączyć do oferty wydruk ze strony**
Wbudowane porty	Wbudowane porty: - 2 x DisplayPort - 1 x HDMI 2.0 - 1 x LAN 10/100/1000 wspierająca obsługę WoL, umożliwiająca zdalny dostęp do wbudowanej sprzętowej technologii zarządzania komputerem. Porty USB : Panel przedni – 4 w USB, w tym 2 x USB 3.2 i 1 x USB typu C; Panel Tylny - 6 x USB, w tym 4 x USB 3.2 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp.

	Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Wszystkie wymagane porty muszą być w sposób stały zintegrowane z obudową (wlutowane w laminat płyty głównej). Płyta główna wyposażona w : - 1 slot PCI Express x16 Gen.3, - 1 slot PCI Express x4 - 4 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 SSD - 1 złącze M.2 WLAN Klawiatura USB w układzie polski programisty Mysz laserowa USB z rolką (scroll) Nagrywarka DVD +/-RW o prędkości min. 8x
Wsparcie techniczne	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera; Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).
Warunki gwarancji i serwisu	3 lata; Serwis musi być realizowany zgodnie z normami ISO 9001 i ISO 27001 – **załączyć do oferty certyfikaty dla Oferenta;** Sposób realizacji usług wsparcia technicznego : ▪ Telefoniczne zgłaszanie usterek w dni robocze w godzinach 8-17. ▪ Dedykowany bezpłatny portal online do zgłaszania usterek i zarządzania zgłoszeniami serwisowymi. Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii. W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy musi przybyć na miejsce instalacji na następny dzien roboczy od momentu przyjęcia zgłoszenia; Mozliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń z nieaktywnym wsparciem technicznym. Dostawca zapewni bezpłatne oprogramowanie do automatycznej diagnostyki i zdalnego zgłaszania awarii.
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:

	a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 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;
Oprogramowanie użytkowe	System chroniący przed zagrożeniami, posiadający certyfikaty: OPSWAT Platinum, AV-Test 'Top Product', AV Comperative Advance +, ISO 27001 . 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 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. Pełne szyfrowanie dysków. 14. Zapobieganie utracie danych z powodu utraty / kradzieży komputera. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępniać je wyłącznie autoryzowanym użytkownikom. 15. Oprogramowanie musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. 16. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej. 17. Możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. 18. Interfejs zarządzania musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. 19. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. 20. Ograniczenie możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. 21. Możliwość zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika. 22. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów musza mieć możliwość modyfikowania plików objętych ochroną any ransomware. 23. Monitorowanie krytycznych danych użytkownika zapewniające zapobiegające przed niezamierzonymi manipulacjami – ataki ransomware 24. Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej: a) Przechowywanie danych w bazie typu SQL; b) Zdalną instalację lub deinstalację oprogramowania na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z

	ActiveDirectory c) Tworzenie paczek instalacyjnych oprogramowania, z rozróżnieniem docelowej platformy systemowej, w tym 32 lub 64bit dla systemów Windows i Linux); d) Centralną dystrybucję uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet; e) Raportowanie dostępne przez konsolę, 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 dane/raporty zbierane ze stacji klienckich, w tym raporty o zainstalowanym oprogramowaniu; f) Definiowanie struktury zarządzania opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji 25. Musi wyświetlać status bezpieczeństwa konsolidacyjnego urządzeń końcowych; 26. Tworzenie kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury 27. Skuteczna polityka lokalna i globalna; 28. Możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp zgodnie z przypisaniem do grupy 29. Dostęp do konsoli z dowolnego miejsca w nagłych przypadkach 30. Możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń 31. Możliwość uzyskania raportów i powiadomień za pomocą poczty elektronicznej 32. 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. 33. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z witryny producenta oprogramowania. 34. Centralna konsola zarządzająca oraz oprogramowanie chroniące serwer 35. Oprogramowanie klienckie zarządzane z poziomu serwera. 36. System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej: a) różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie b) przyznane praw dostępu dla nośników pamięci tj. USB, CD c) egulowanie połączeń WiFi i Bluetoot d) kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe e) blokadę lub zezwolenie na połączenie się z urządzeniami mobilnymi f) blokowanie dostępu dowolnemu urządzeniu g) możliwość tymczasowego dodania dostępu do urządzenia przez administratora h) szyfrowanie zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu i) możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka

	j) zezwalanie na dostęp tylko urządzeniom wcześniej dodanym przez administratora k) używanie tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich l) funkcję wirtualnej klawiatury m) możliwość blokowania każdej aplikacji n) możliwość zablokowania aplikacji w oparciu o kategorie o) możliwość dodania własnych aplikacji do listy zablokowanych p) zdolność do tworzenia listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze q) możliwość wyboru pojedynczej aplikacji w konkretnej wersji 37. Kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool 38. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. 39. Możliwość zablokowania funkcji Printscreen 40. Monitorowanie przesyłu danych między aplikacjami; 41. Monitorowanie i kontrola przepływu poufnych informacji 42. Możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików 43. Możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj 44. Możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe 45. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe 46. Ochrona zawartości schowka systemu 47. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL 48. Możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych 49. Ochrona plików zamkniętych w archiwach 50. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem 51. Możliwość tworzenia profilu DLP dla każdej polityki 52. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania 53. Ochrona przez wyciekiem plików poprzez programy typu p2p 54. Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. 55. Monitorowania określonych rodzajów plików. 56. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. 57. Generator raportów o funkcjonalności monitora zmian w plikach. 58. Możliwość śledzenia zmian we wszystkich plikach 59. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach 60. Możliwość definiowana własnych typów plików 61. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku 62. Optymalizacja w startu systemu operacyjnego, przed jego całkowitym

	uruchomieniem 63. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich 64. System ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochrona; 65. Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej. 66. Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email 67. Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika 68. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi 69. Musi posiadać możliwość eksportu danych użytkownika 70. Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO 71. Musi umożliwiać import listy urządzeń z pliku CSV 72. Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, grupa, reguły, wersja agenta; 73. Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przestrzeń na dysku, bateria, zużycie procesora, sygnał 74. Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni; 75. Musi zawierać podgląd aktualnie zainstalowanych aplikacji 76. Musi zawierać informacje o zużyciu łącza danych, a w tym: ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, 77. Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł 78. Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres; 79. Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa: 80. Dostęp za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową 81. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta. 82. Dostęp do portalu zarządzającego za pomocą wspieranych przeglądarek internetowych: - Microsoft Internet Explorer, - Microsoft Edge, Mozilla Firefox, Google Chrome, Safari; 83. Skany podatności za pomocą dedykowanych nodów skanujących; 84. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 85. Portal zarządzający musi umożliwiać: a) przegląd wybranych danych b) zablokowania możliwości zmiany konfiguracji widgetó c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych

	skanów podatności e) eksport wszystkich skanów podatności do pliku CSV 86. Backup i przywracanie danych; 87. Deduplikacja danych, 88. Backup przyrostowy i różnicowy, 89. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, 90. Backup danych lokalnych – plikowy oraz poczty Outlook, 91. Backup otwartych plików (VSS), 92. Filtr plików oraz folderów, 93. Domyślne wykluczenia zbędnych plików (pliki tymczasowe), 94. Wyłączanie komputera po wykonaniu backupu, 95. Przywracanie danych do wskazanej lokalizacji, 96. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora, 97. Wyszukiwanie plików w repozytorium użytkownika, 98. Automatyczne logowanie, 99. Zapamiętywanie danych logowania, 100. Automatyczne uruchamianie programu przy starcie systemu, 101. Ustawianie priorytetu dla procesu backupu, 102. Zmiana klucza szyfrującego, 103. Ustawienia przepustowości/zajętości pasma, 104. Konfiguracja wydajności procesu backupu, 105. Zastępowanie nazwy pliku GUID-em, 106. Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika, 107. Kompresja danych, 108. Transmisja po bezpiecznym protokole TLS, 109. Deklaracja klucza szyfrującego dane użytkownika, 110. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, 111. Obliczanie sumy kontrolnej, 112. Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB; 113. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte w cenie licencji; 114. Oprogramowanie producenta komputera z nieograniczoną czasowo licencją na użytkowanie umożliwiające: a) upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności do najnowszej dostępnej wersji, b) sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi c) dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne d) włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji e) sprawdzenie historii aktualizacji z informacją, jakie sterowniki były instalowane z dokładną datą i wersją (rewizja wydania)

	f) dostęp do wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu; g) dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu; 115. Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku.

II. Skaner – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ	Płaski i ADF;
Tryby skanowania	Jednostronnie i dwustronnie, mono i kolor;
Czujniki skanowania	2 x CIS
Źródłow światła	2 x LED RGB
Rozmiar dokumentu	Skaner płaski 220 – 290 mm, ADF – 220 – 350 mm;
Szybkość skanowania	Skaner płaski 4s./str., ADF – 25 str/min - simpleks, 50 obr./min. - dupleks
Pojemnośc ADF	50 arkuszy A4;
Maksymalnye dzienny nakład zalecany przez producenta	4000 arkuszy;
Rozdzielczość	600 dpi;
Interfejs	USB;
Procesowanie obrazu	Podkreślenie obrazu, rozpraszanie błędów i koloru, dynamiczny i statyczny próg, DTC, SDTC, derasteryzacja, kolor odrzucany, automatyczne wykrywanie koloru, drukowanie wielu obrazów, wykrywanie pustych stron, podzielony obraz, redukcja pionowych smug, wypełnianie krawędzi, automatyczne wykrywanie rozmiaru strony;
Zuzycie energii przy pracy	Maksymalnie 20 W;
Wymagania dodatkowe	Współpraca z posiadanymi przez zamawiającego systemami Windows 10 i 11 Pro, programowy panel sterowania, separator arkuszy, kabel USB, godnośc z EnergyStar i RoHs;

III. Zestaw serwea NAS – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Procesor	Musi osiagać wynik 5250 wteście Average CPU Mark – **załaczyć do oferty wydruk ze strony** www.cpunechmark.net
Pamięć	8 GB możliwoscia rozbudowy do 64 GB;;
Pamięc flash	5 GB;
Zatoki na dyski	6 szt.;
Obsługiwane dyski	2,5 oraz 3,5 cala SAS i SATA;, hot swap;
Porty	2 z 2,5 GbE; 3 x USB 10 Gbps, 1 x USB 5 Gbps;

	1 x PCIe; 2 x M.2
Diody	USB, zasilanie, LAN, zatoki dyskowe, złącza M.2;
Wentylatory	3 szt.
CIFS	2000;
Rozmiar puli	300 TB;
Ilość pul	128
Zainstalowane dyski	5 x 4 TB SATA 6 Gb/s, przeznaczone do pracy w trybie ciągłym w serwerach NAS; MTBF – 1 mln. godzin, Głośność – maksymalnie 30 dB Wbudowane kolejkowanie poleceń; Współczynnik obciążenia praca – 180 TB/rok; Pamięc podręczna – 128 MiB;
Pobór mocy podczas pracy	Maksymalnie 50W;
Zasilacz	Moc – 700W; Gniazda – 5 x FR; Czas transferu – maksymalnie 5 ms. Podtrzymanie na baterii – 12 s. przy połowie obciążenia i 4 s. przy pełnuym obciążeniu; Układ przeciwprzepięciowy – 450J; Hałas – 50dB; Gwarancja – 2 lata;
System operacyjny	1. Obsługa zbiorczego tworzenia użytkowników przez importowanie list użytkowników; 2. Obsługa dodawania użytkowników do więcej niż jednej grupy użytkowników; 3. Obsługa konfiguracji siły hasła i reguł wygaśnięcia 4. Możliwość samodzielnego resetowania hasła w przypadku użytkowników niebędących administratorami 5. Możliwość dostosowania uprawnień dla poszczególnych folderów i plików dla użytkowników i grup 6. Możliwość dostosowania ustawień uprawnień aplikacji dla użytkowników, grup i adresów IP 7. Obsługa limitów konfiguracji wolumenów/folderów współdzielonych w celu kontrolowania maksymalnej ilości miejsca dostępnego dla każdego użytkownika 8. Obsługa limitów szybkości dla użytkowników i grup dla protokołów FTP; 9. SSD TRIM; 10. Wsparcie dla grup RAID; 11. Wparcie dla RAID 0,1,5,6,10, F1, JBOD; 12. Migracja z RAID 1 do 5 i z 5 do 6; 13. Możliwość powiększenia wolumenu przez dodanie kolejnych dysków lub zamianę dysków mniejszych na większe; 14. Obsługa FTP, FTP przez SSL/TLS i SFTP; 15. Ustawienia limitu czasu rozłączania bezczynnych użytkowników 16. Mozliwość dostosowania zakresów portów dla pasywnych połączeń FTP;

	17. Transfer plików między serwerami; 18. Ustawienia ograniczeń połączeń dla adresów IP 19. Ustawienia limitu prędkości dla określonych użytkowników lub grup; 20. Obsługa trybu transferu ASCII 21. Obsługa kodowania UTF-8 dla plików z wielojęzycznymi nazwami 22. Katalog główny dla każdego użytkownika 23. Anonimowy FTP; 24. Obsługa protokołu SSH podczas przesyłania plików; 25. Synchronizacja folderów współdzielonych; 26. Kopia zapasowa jednostek LUN 27. Zarządzanie pamięcią masową i monitorowanie użycia pamięci masowej serwera; 28. Obsługa migawek i tworzenia zadań replikacji dla folderów współdzielonych i jednostek LUN 29. Przeglądanie migawek tylko do odczytu 30. Menedżer plików do przeglądania i zarządzania folderami i plikami przechowywanymi na serwerze; 31. Bezpieczne udostępnianie plików 32. Dostęp i zarządzanie z komputerów osobistych, tabletów i telefonów komórkowych; 33. Montowanie dysków wirtualnych, folderów zdalnych i pamięci masowej w chmurze publicznej; 34. Odzyskiwanie lub pobieranie usuniętych plików z kosza 35. Wyświetlanie i dostosowywanie uprawnień ACL do plików i folderów; 36. Obsługa edytora ACL 37. Dostosowywanie atrybutów folderów współdzielonych do wyświetlania; 38. Kompresowanie lub wyodrębnianie zarchiwizowanych plików i folderów; 39. Montowanie dysków wirtualnych w celu uzyskania dostępu do zawartości plików obrazów dysków (.iso 40. Montowanie folderów zdalnych ze zdalnych serwerów obsługujących protokoły SMB1/SMB2/SMB3/NFS 41. Łączenie ze zdalnymi usługami chmury publicznej i serwerami plików; 42. Obsługiwane protokoły: FTP, SFTP, WebDAV, WebDAV HTTPS 43. Centralne zarządzanie za pośrednictwem menedżera łączy udostępnionych; 44. Logi transferu plików i działań użytkownika z możliwościa eksportu;
Warunki gwarancji	3 lata;
Wymagania dodatkowe	Kensington lock, obsługa jumbo frame, funkcja Wake on LAN / WAN;

IV. Monitory – 17 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;

V. Urządzenia wielofunkcyjne – 12 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ drukarki	Laser, mono
Funkcje	Drukowanie, kopiowanie, skanowanie;
Pamięć	128MB
Procesor	600MHz
Komunikacja	Siec LAN, port USV;
Rozdzielczość kopiowania/ drukowania	600 x 600 dpi / 1200 x 1200 dpi;
Szybkość druku/kopiowania	30 str./min.
Szybkośc dupleksu	15 str. /min.
Zużycie energii druk	Maksymalnie 480W;
Poziom hałasu druk	Maksymalnie 50 dB;
Obsługa nosników	A4, A5, A6;
Podajnik paieru	250 arkuszy
Odbiornik papieru	100 arkuszy;
Rozdzielczość skanowania	1200 x 1200 dpi;
Szybkość skanowania mono/kolor	20/7 obrazów/min
Warunki gwarancji	3 lata;
Wymagania dodatkowe	Dupleks, ADF, kompatybilność z posiadanymi przez zamawiającego systemami Windows 10, toner na 2 i będen na 12 tys. stron;

VI. 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
Ekran	15.6” FHD (1920 x 1080) powłoka przeciwodblaskowa, jasność 250 nits, kontrast 700:1;
Wydajność	Oferowany komputer musi osiągać w teście wydajności BAPCO Sysmark 25 wynik 1300 pkt. **Wydruk z oprogramowania testującego 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.). Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego
Pamięć RAM	16GB DDR4 i możliwość rozbudowy do 32GB, 2 sloty na pamięci
Pamięć masowa	500GB NVMe SSD; Fabryczna możliwość instalacji dwóch dysków PCIe.
Grafika	Osiągająca w teście Sysmark25 Creativity co najmniej 1100 punktów. **Wydruk z oprogramowania testującego 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.). Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego
Klawiatura	Klawiatura w standardzie US, wydzieloną klawiaturą numeryczną i wbudowanym w klawiaturze podświetleniem. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12.
Multimedia	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo o mocy 2x 2W. Dwa kierunkowe, cyfrowe mikrofony z funkcją redukcji szumów i poprawy mowy wbudowane w obudowę matrycy.

	Kamera internetowa z diodą informującą o aktywności, 720p, trwale zainstalowana w obudowie matrycy wyposażona w mechaniczną przysłonę. Czytnik kart micro SD, 1 port audio typu combo (słuchawki i mikrofon)
Łączność bezprzewodowa	Karta Wi-Fi 5 AX + Bluetooth Możliwość instalacji wewnętrznego modelu LTE
Bateria i zasilanie	40Whr umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Zasilacz o mocy 65W TYP-C/thunderbolt
Waga i wymiary	Waga maksymalnie 1,70 z baterią
Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane; Dookoła matrycy uszczelnienie chroniące klawiaturę po zamknięciu przed kurzem i wilgocią. Kąt otwarcia notebooka min 180 stopni. Komputer spełniający normy MIL-STD-810H lub równoważne – **załączyć do oferty potwierdzające materiały producenta;**
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 informacj: data produkcji komputera, o kontrolerze audio, procesorze, a w szczególności osiągana prędkość, pamięci RAM z informacją o taktowaniu i obsadzeniu w slotach. Niezmazywalne i nieedytowalne pole asset tag z możliwością wpisywania znaków specjalnych. Funkcje logowania się do BIOS na podstawie hasła systemowego/użytkownika, administratora ; Blokowanie hasłem systemowym/użytkownika dostępu do dysku twardego, Funkcja umożliwiająca założenie hasła na dysk, uzyskanie informacji o stanie naładowania baterii, podpiętego zasilacza; Zarządzanie trybem ładowania baterii, w tym określenie docelowego poziomu naładowania; Możliwość nadania numeru inwentarzowego z poziomu BIOS bez wykorzystania dodatkowego oprogramowania, jak i konieczności aktualizacji BIOS; Możliwość włączenia/wyłączenia funkcji automatycznego tworzenia recovery BIOS na dysku twardym.
Certyfikaty	Laptop musi być wyprodukowany zgodnie z normami ISO9001 i ISO50001 – **certyfikaty załączyć do oferty;**
Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. Działający w pełni, bez okrojonych funkcjonalności nawet w przypadku uszkodzonego dysku, braku dysku lub sformatowanym dysku, dostępu do sieci i internetu oraz bez konieczności podłączenia urządzeń wewnętrznych i zewnętrznych.
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. Wbudowany czyjnik otwarcia obudowy (dolnej pokrywy) Czytnik linii papilarnych
Zarządzanie zdalne	Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca: 1. Monitorowanie konfiguracji komponentów komputera - CPU, Pamięć, HDD wersja BIOS płyty głównej; 2. Zdalną konfigurację ustawień BIOS, 3. Zdalne przejęcie konsoli tekstowej systemu;; 4. Przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM z serwera zarządzającego; 5. Zdalne przejecie pełnej konsoli graficznej systemu tzw. KVM Redirection bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 1920x1080 włącznie; 6. Zapis i przechowywanie dodatkowych informacji o wersji zainstalowanego oprogramowania i zdalny odczyt tych informacji 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/) Nawiązywanie zdalnego szyfrowanego połączenia z serwerem zarządzającym, w definiowanych odstępach czasu, w przypadku wystąpienia zdarzenia lub błędu systemowego oraz na żądanie użytkownika z poziomu BIOS. Wbudowany sprzętowo log operacji zdalnego zarządzania, możliwy do kasowania tylko przez upoważnionego użytkownika; Sprzętowy firewall zarządzany i konfigurowany z serwera zarządzania oraz niedostępny dla lokalnego systemu operacyjnego i lokalnych aplikacji; Konsola zarządzania wyświetlająca informacje i zachowująca pełną funkcjonalność nawet podczas restartów komputer;.
Wbudowane porty i złącza	1 x HDMI 2.0, 1 x RJ-45, 2 x USB 3.2 w tym jeden port z zasilaniem, 2 x Thunderbolt 4, złącze na linkę zabezpieczającą.
Warunki gwarancyjne	3-letnia gwarancja producenta świadczona na miejscu u klienta; Czas reakcji serwisu - do końca następnego dnia roboczego. Serwis musi być realizowany zgodnie z normami ISO 9001 i ISO 27001 – **załączyć do oferty certyfikaty dla Oferenta** Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta, w tym: automatyczna identyfikacja komputera, rodzaj gwarancji, data produkcji komputera, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego)
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:

	a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 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;
Oprogramowanie użytkowe	System chroniący przed zagrożeniami, posiadający certyfikaty: OPSWAT Platinum, AV-Test 'Top Product', AV Comperative Advance +, ISO 27001. 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 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. Pełne szyfrowanie dysków. 14. Zapobieganie utracie danych z powodu utraty / kradzieży komputera. Oprogramowanie musi szyfrować całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępniać je wyłącznie autoryzowanym użytkownikom. 15. Oprogramowanie musi umożliwiać blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. 16. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej. 17. Możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. 18. Interfejs zarządzania musi wyświetlać monity o zbliżającym się zakończeniu licencji, a także powiadamiać o zakończeniu licencji. 19. Moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. 20. Ograniczenie możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. 21. Możliwość zdefiniowania chronionych folderów zawierających wrażliwe dane użytkownika. 22. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów musza mieć możliwość modyfikowania plików objętych ochroną any ransomware. 23. Monitorowanie krytycznych danych użytkownika zapewniające zapobiegające przed niezamierzonymi manipulacjami – ataki ransomware 24. Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej: a) Przechowywanie danych w bazie typu SQL; b) Zdalną instalację lub deinstalację oprogramowania na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z

	ActiveDirectory c) Tworzenie paczek instalacyjnych oprogramowania, z rozróżnieniem docelowej platformy systemowej, w tym 32 lub 64bit dla systemów Windows i Linux); d) Centralną dystrybucję uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet; e) Raportowanie dostępne przez konsolę, 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 dane/raporty zbierane ze stacji klienckich, w tym raporty o zainstalowanym oprogramowaniu; f) Definiowanie struktury zarządzania opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji 25. Musi wyświetlać status bezpieczeństwa konsolidacyjnego urządzeń końcowych; 26. Tworzenie kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury 27. Skuteczna polityka lokalna i globalna; 28. Możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp zgodnie z przypisaniem do grupy 29. Dostęp do konsoli z dowolnego miejsca w nagłych przypadkach 30. Możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń 31. Możliwość uzyskania raportów i powiadomień za pomocą poczty elektronicznej 32. 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. 33. Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z witryny producenta oprogramowania. 34. Centralna konsola zarządzająca oraz oprogramowanie chroniące serwer 35. Oprogramowanie klienckie zarządzane z poziomu serwera. 36. System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej: a) różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowani b) przyznane praw dostępu dla nośników pamięci tj. USB, CD c) regulowanie połączeń WiFi i Bluetoot d) kontrolowanie i regulowanie użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe e) blokadę lub zezwolenie na połączenie się z urządzeniami mobilnymi f) blokowanie dostępu dowolnemu urządzeni g) możliwość tymczasowego dodania dostępu do urządzenia przez administratora h) szyfrowanie zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu i) możliwość zablokowania funkcjonalności portów USB, blokując dostęp

	urządzeniom innym niż klawiatura i myszka j) zezwalanie na dostęp tylko urządzeniom wcześniej dodanym przez administratora k) używanie tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich l) funkcję wirtualnej klawiatury m) możliwość blokowania każdej aplikacji n) możliwość zablokowania aplikacji w oparciu o kategorie o) możliwość dodania własnych aplikacji do listy zablokowanych p) zdolność do tworzenia listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze q) możliwość wyboru pojedynczej aplikacji w konkretnej wersji 37. Kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool 38. Możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki. 39. Możliwość zablokowania funkcji Printscreen 40. Monitorowanie przesyłu danych między aplikacjami; 41. Monitorowanie i kontrola przepływu poufnych informacji 42. Możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików 43. Możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj 44. Możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe 45. Ochrona przed wyciekiem informacji na drukarki lokalne i sieciowe 46. Ochrona zawartości schowka systemu 47. Ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL 48. Możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych 49. Ochrona plików zamkniętych w archiwach 50. Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem 51. Możliwość tworzenia profilu DLP dla każdej polityki 52. Wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania 53. Ochrona przez wyciekiem plików poprzez programy typu p2p 54. Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych. 55. Monitorowania określonych rodzajów plików. 56. Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania. 57. Generator raportów o funkcjonalności monitora zmian w plikach. 58. Możliwość śledzenia zmian we wszystkich plikach 59. Możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach 60. Możliwość definiowana własnych typów plików 61. Usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku

	62. Optymalizacja w startu systemu operacyjnego, przed jego całkowitym uruchomieniem 63. Możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich 64. System ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochrona; 65. Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej. 66. Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email 67. Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika 68. Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi 69. Musi posiadać możliwość eksportu danych użytkownika 70. Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO 71. Musi umożliwiać import listy urządzeń z pliku CSV 72. Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, grupa, reguły, wersja agenta; 73. Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przestrzeń na dysku, bateria, zużycie procesora, sygnał 74. Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni; 75. Musi zawierać podgląd aktualnie zainstalowanych aplikacji 76. Musi zawierać informacje o zużyciu łącza danych, a w tym: ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych, 77. Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł 78. Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres; 79. Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa: 80. Dostęp za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową 81. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta. 82. Dostęp do portalu zarządzającego za pomocą wspieranych przeglądarek internetowych: - Microsoft Internet Explorer, - Microsoft Edge, Mozilla Firefox, Google Chrome, Safari; 83. Skany podatności za pomocą dedykowanych nodów skanujących; 84. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 85. Portal zarządzający musi umożliwiać: a) przegląd wybranych danych; b) zablokowanie możliwości zmiany konfiguracji widgetów c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.

	d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności e) eksport wszystkich skanów podatności do pliku CSV 86. Backup i przywracanie danych; 87. Deduplikacja danych, 88. Backup przyrostowy i różnicowy, 89. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, 90. Backup danych lokalnych – plikowy oraz poczty Outlook, 91. Backup otwartych plików (VSS), 92. Filtr plików oraz folderów, 93. Domyślne wykluczenia zbędnych plików (pliki tymczasowe), 94. Wyłączanie komputera po wykonaniu backupu, 95. Przywracanie danych do wskazanej lokalizacji, 96. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora, 97. Wyszukiwanie plików w repozytorium użytkownika, 98. Automatyczne logowanie, 99. Zapamiętywanie danych logowania, 100. Automatyczne uruchamianie programu przy starcie systemu, 101. Ustawianie priorytetu dla procesu backupu, 102. Zmiana klucza szyfrującego, 103. Ustawienia przepustowości/zajętości pasma, 104. Konfiguracja wydajności procesu backupu, 105. Zastępowanie nazwy pliku GUID-em, 106. Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika, 107. Kompresja danych, 108. Transmisja po bezpiecznym protokole TLS, 109. Deklaracja klucza szyfrującego dane użytkownika, 110. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, 111. Obliczanie sumy kontrolnej, 112. Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB; 113. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte w cenie licencji; 114. Oprogramowanie producenta komputera z nieograniczoną czasowo licencją na użytkowanie umożliwiające: a) upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności do najnowszej dostępnej wersji, b) sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi c) dostęp do wykazu najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne d) włączenie/wyłączenie funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji e) sprawdzenie historii aktualizacji z informacją, jakie sterowniki były

	instalowane z dokładną datą i wersją (rewizja wydania) f) dostęp do wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu; g) dostęp do raportu uwzględniającego informacje o znalezionych, pobranych i zainstalowanych aktualizacjach z informacją, jakich komponentów dotyczyły, możliwość exportu takiego raportu; 115. Raport musi zawierać datę i godzinę podjętych i wykonanych akcji/zadań w przedziale czasowym min. 1 roku.

VII. Pamięć USB – 4 szt.

1. Pojemność – 32 GB
2. Podwójne hasło oraz podwójny system operacyjny;
3. Szyfrowanie sprzętowe wszystkich przechowywanych danych;
4. 256-bitowe, sprzętowe szyfrowanie AES;
5. Wodoszczelna konstrukcja zgodna z normą IEC 60529 IPX8;
6. Stalowa obudowa wewnętrzna i gumowana obudowa zewnętrzna;
7. Ochrona danych w razie upuszczenia, zgniecenia i zanurzenia urządzenia w wodzie;
8. Dostęp lub usunięcie danych nie może być możliwe bez podania poprawnego hasła;
9. Możliwosc ustawienia hasła o długości 8-16 znaków;
10. Po sześciu nieudanych próbach uzyskania dostępu dane musza być kasowane;
11. Po skasowaniu danych, urządzenie musi być gotowe do ponownego użytku
12. Funkcja identyfikacji właściciela;
13. W razie zgubienia urządzenia, dane kontaktowe musza być dostępne w pamięci urządzenia;
14. Brak potrzeby instalacji oprogramowania
15. Zainstalowany interfejs użytkownika w 22 językach
16. Złącze – USB;
17. Odczyt/zapis - 17/14 MB/s.
18. Kompatybilność z posiadanymi przez zamawiającego systemami Windows 7,8,8.1,10;
19. Zgodność z ustawą o RODO;
20. Wszystkie dane przechowywane na pamięci musza być są szyfrowane. Ta funkcja nie może być wyłączane przez użytkownika;
21. Ochrona przed atakami za pomocą hasła Brute-Force;
22. Urzadzenie musi się szyfrować wraz zwyjąciem z urządzenia;
23. Administrator musi mieć możliwość skonfigurowania własnego hasła oraz hasła użytkownika
24. Musi być zabezpieczony przed manipulacją, rozebraniem i sklonowaniem;
25. Musi być wodoodporny, pyłoszczelny i odporny na wstrząsy;

VIII. System autentykacji – 70 szt.

1 Urządzenia autoryzacyjne do systemu operacyjnego lub serwera kontrolera domeny;
2 Wsparcie techniczne i prawo do aktualizacji na rok.
3 Uwierzytelnienie użytkowników do systemu operacyjnego lub serwera kontrolera domeny przy pomocy dedykowanego urządzenia sprzętowego;
4 Monitorowania logów uwzględniające:
  4.1 logowanie do systemu (kto, kiedy)
  4.2 wylogowanie/zablokowanie systemu (kto, kiedy)
5 Użytkownik zanim dokona logowania do systemu operacyjnego przy pomocy urządzenia

sprzętowego musi mieć możliwość wyświetlenia zdefiniowanej przez administratora wewnętrznej PBI.

6 Administrator Bezpieczeństwa Informacji mmusi mieć możliwość zarządzania treścią, która jest wyświetlana i akceptowana w procesie logowania do systemu operacyjnego lub kontrolera domeny.

7 Użytkownik, który opuszcza stanowisko pracy będzie musi mieć blokowany system operacyjny przez urządzenie sprzętowe.

8 Pamięć urządzenia sprzętowego musi umożliwiać zdefiniowania 20 uwierzytelnień do systemu operacyjnego.

9 Możliwość autoryzacji do systemu operacyjnego lub kontrolera domeny dedykowanym PIN-em.

10 Możliwość nadawania indywidualnego kodu PIN do urządzenia autoryzacyjnego dla konta użytkownika w systemie operacyjnym lub kontrolerze domeny.

11 Zastosowane urządzenie sprzętowe musi umożliwiać przypisywanie konkretnego komputera do urządzenia sprzętowego.

12 Narzędzie sprzętowe musi wykorzystywać tylko jeden port USB w wersji 2.0 lub 3.0

13 Urządzenie autoryzacyjne TOKEN musi komunikować się w celu autoryzacji z urządzeniami wyposażonymi w interfejs NFC.

14 Urządzenie sprzętowe w celu uwierzytelnienia musi wymagać stosowania 6 znakowego PIN-u,

15 System musi współpracować co najmniej z posiadnymi przez zamawiającego systemami operacyjnymi Windows 7,8,8.1,10

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.