Opis przedmiotu zamówienia dla części 1 pn. „Zakup i dostawa komputerów PC, laptopów oraz oprogramowania w ramach projektu Cyfrowa Gmina”

Komputer stacjonarny PC – 35 szt.

Rodzaj komponentu	**Wymagane minimalne parametry techniczne komputera**
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 – wynik min. 1100. Wynik testu należy oświadczyć w formularzu ofertowym 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 konfiguracją) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.) Zamawiający zastrzega sobie prawo do wykonania testu SYSMARK 25 na etapie odbioru na losowo wybranej 10% próbie. Odbiór nastąpi po pozytywnym osiągnięciu wyniku przetestowanego sprzętu
Pamięć operacyjna	Min. 16GB DDR4 z możliwością rozbudowy do 64GB
Parametry pamięci masowej	Min. 1x 256GB SSD
Grafika	Zintegrowana ze wsparciem dla DirectX 12
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, min. 2 kanałowa
Obudowa	Obudowa zaprojektowana i wykonana na zlecenie producenta komputera Możliwość montażu niskoprofilowych kart graficznych, montaż beznarzędziowy dysku 3,5" oraz 2,5”, napędu optycznego i kart rozszerzeń Obudowa wykonana z wytrzymałego tworzywa, blachy o grubości co najmniej 0,6mm Możliwość montażu dysku 2,5" oraz 3,5" wewnątrz obudowy Zatoki na dyski i napędy: 2× 2,5/3,5, 1× 3,5, 1x 5,25 (typ Slim) Wyposażona w co najmniej 2 porty 3.1 oraz złącza mikrofonu i słuchawek z przodu obudowy Wbudowana karta sieciowa 10/100/1000 Możliwość otwierania bez użycia narzędzi (wkręty ręczne) Wyposażona w Kensington Lock i ucho na kłódkę Zasilacz o mocy minimum 300W 80+ Bronze Zasilacz w oferowanym komputerze musi znajdować się na stronie internetowej http://www.plugloadsolutions.com/80pluspowersupplies.aspx W obudowie zamontowane trzy fabrycznie filtry przeciwkurzowe, umiejscowione na froncie, pod zasilaczem oraz na topie obudowy Obudowa wyposażona w trzystopniowy kontroler obrotów na w sumie 6 wentylatorów
Certyfikaty i standardy	Deklaracja zgodności CE Poprawna praca z oprogramowaniem Microsoft – dołączyć Windows hardware certification report Produkcja sprzętu zgodnie z ISO 9001, ISO 27001, ISO 28000 Oprogramowanie producenta komputera umożliwiające zdalną i lokalną administrację oferowanych komputerów oraz ich diagnostykę, pozwalające na: - zdalną i lokalną inwentaryzację komponentów komputera - zdalne i lokalne monitorowanie stanu komponentów: CPU, Pamięć RAM, HDD, wersje BIOS

	- zdalne włączenie, wyłączanie oraz restart komputera w sieci - monitorowanie i alertowanie temperatur, napięć i zajętości dysków twardych wraz z graficznym przedstawieniem wartości w zadanym czasie w postaci wykresów - otrzymywanie informacji WMI – Windows Management Interface Interfejs komunikacyjny ww. oprogramowania musi być w języku polskim. W celu zapewnienia pełnej kompatybilności ww. oprogramowania z komputerem, ww. oprogramowanie musi być wyprodukowane w całości przez producenta komputera. Nie dopuszcza się zaoferowania ww. oprogramowania, składającego się z kilku różnych programów, wyprodukowanych przez różnych producentów, które sumarycznie spełniałby ww. wymagania
Oprogramowanie antywirusowe	W wyniku rekomendacji z dnia 9 maja 2022 r. wydanej przez Kolegium do Spraw Cyberbezpieczeństwa w sprawie niestosowania w systemach informacyjnych oprogramowania, którego producentem jest Kaspersky Lab z siedzibą w Moskwie (Federacja Rosyjska), na które składa się w szczególności oprogramowanie: Kaspersky Internet Security, Kaspersky Anti-Virus, Kaspersky TOTAL Security oraz Kaspersky Safe Kids, ze względu na stwierdzony negatywny wpływ tego oprogramowania na bezpieczeństwo publiczne nie dopuszcza się stosowania w/w oprogramowania System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej: - wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji - wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych - wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej. Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom Zarządzanie przez Chmurę: - musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach - musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury - musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur - musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy - musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer Oprogramowanie klienckie, zarządzane z poziomu serwera System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej: - różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie - funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD

	- funkcje regulowania połączeń WiFi i Bluetooth - funkcje blokowania dostępu dowolnemu urządzeniu - zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu - możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka Monitorowanie zmian w plikach: - możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych - funkcje monitorowania określonych rodzajów plików - możliwość wykluczenia określonych plików/folderów dla procedury monitorowania - generator raportów do funkcjonalności monitora zmian w plikach - możliwość śledzenia zmian we wszystkich plikach - możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach - możliwość definiowana własnych typów plików Optymalizacja systemu operacyjnego stacji klienckich: - usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku - optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem - możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich - instruktaż stanowiskowy pracowników Zamawiającego - dokumentacja techniczna w języku polskim Moduł oprogramowania pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa - wymagania dotyczące technologii: - dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową - portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta - dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych - rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących - nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie Portal zarządzający musi umożliwiać: - przegląd wybranych danych na podstawie konfigurowalnych widgetów - zablokowania możliwości zmiany konfiguracji widgetów - zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów - tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności - eksport wszystkich skanów podatności do pliku CSV Backup i przywracanie danych (licencja wieczysta): - deduplikacja danych - backup przyrostowy i różnicowy - wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji - backup danych lokalnych – plikowy oraz poczty outlook - backup otwartych plików (vss) - filtr plików oraz folderów - domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.), - wyłączanie komputera po wykonaniu backupu - przywracanie danych do wskazanej lokalizacji - możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora - wyszukiwanie plików w repozytorium użytkownika Ustawienia: - automatyczne logowanie - zapamiętywanie danych logowania - automatyczne uruchamianie programu przy starcie systemu - ustawianie priorytetu dla procesu backupu

	- zmiana klucza szyfrującego - ustawienia przepustowości/zajętości pasma - konfiguracja wydajności procesu backupu Bezpieczeństwo: - zastępowanie nazwy pliku guid-em - szyfrowanie danych algorytmem aes 256 cbc, zawsze po stronie komputera użytkownika - kompresja danych - transmisja po bezpiecznym protokole tls - deklaracja klucza szyfrującego dane użytkownika - szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji - obliczanie sumy kontrolnej - kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center na terenie Polski. WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 10 i nowsze, Mac OS,Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Wsparcie techniczne, świadczone w języku polskim, zawarte jest w cenie licencji
BIOS	BIOS zgodny ze specyfikacją UEFI Możliwość obsługi klawiaturą oraz myszą Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - wersji BIOS - nr seryjnym komputera - ilości pamięci RAM - typie procesora - pojemności zainstalowanego dysku twardego - rodzajach napędów optycznych - kontrolerze audio Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń BIOS ma być w pełni obsługiwany przez interfejs myszy i klawiatury oraz w pełni wykorzystywać dyski twarde większe niż 2.2TB
System operacyjny	Windows 10 Professional lub Windows 11 Professional
Wymagania dodatkowe	Wbudowane porty: - min. 1 x DVI lub VGA - min. 1 x HDMI ver. 1.4 - min. 6 portów USB wyprowadzonych na zewnątrz komputera w tym min.: min. 2 porty USB 3.2 z przodu obudowy, 4szt. USB 3.2 z tyłu obudowy - wymagana ilość i rozmieszczenie portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, kart PCIe itp. - porty słuchawek i mikrofonu na przednim oraz tylnym panelu obudowy Komputer musi umożliwiać jego rozbudowę w postaci dedykowanych kart PCIe np. kartę WiFi a/b/g/n Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), PXE 2.1 Płyta główna posiadająca chipset rekomendowany przez producenta procesora, zbudowana w oparciu o kondensatory polimerowe o podwyższonej trwałości przeznaczona dla danego urządzenia; wyposażona w : - SATA III (6 Gb/s) - 4 szt. - M.2 - 2szt. - PCIe 3.0 x16 - 1 szt. - PCIe 3.0 x1 - 2szt. - 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, z obsługą DDR4-3200 MHz Klawiatura USB w układzie polski programisty Mysz USB z klawiszami oraz rolką (scroll)

	Wbudowana w obudowę nagrywarka DVD +/-RW szybkość min. x24 wraz z oprogramowaniem do nagrywania i odtwarzania płyt Wsparcie dla konfiguracji RAID Wbudowany w płytę główną układ przetwarzania energii, zapewniający możliwość całościowego zarządzania poziomem zużywanej energii poprzez wykrywanie aktualnego poziomu wykorzystania zasobów PC (CPU, GPU, HDD, zasilacza) oraz inteligentne przydzielanie mocy w czasie rzeczywistym. Układ działający automatycznie od momentu uruchomienia komputera Ochrona przed nadmiernym napięciem zasilania: System zasilania chroniący obwód specjalnie zaprojektowany przez producenta płyty głównej z wbudowanymi regulatorami napięcia do ochrony chipsetu, gniazd połączeniowych i kodeków audio przed uszkodzeniem spowodowanym nieoczekiwanymi napięciami wysokiej wartości z niestabilnych albo złych zasilaczy

Laptop – 4 szt.

Nazwa	Wymagane parametry techniczne
Zastosowanie	Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej
Przekątna Ekrenu	15.6 FHD IPS (1920 x 1080), powłoką przeciwodblaskową, jasność 220 nits. Kąt otwarcia matrycy min.140 stopni
Wydajność komputera	Oferowany komputer przenośny musi osiągać w teście wydajności: PC Mark10 – wynik min. 3000 punktów. Wynik testu należy oświadczyć w formularzu ofertowym Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora 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 prawo do wykonania testu PC MARK10 na etapie odbioru na losowo wybranej 10% próbie. Odbiór nastąpi po pozytywnym osiągnięciu wyniku przetestowanego sprzętu
Pamięć RAM	Min. 16GB DDR4 2666MHz z możliwością rozbudowy do min. 16GB RAM (nie dopuszcza się pamięci RAM wlutowanych w płytę główną).
Pamięć masowa	256GB NVMe SSD M.2 Komputer musi oferować montaż dwóch dysków w konfiguracji M.2 + 2,5
Karta graficzna	Zintegrowana karta graficzna osiągająca w teście PC Mark 10 Digital Content Creation co najmniej 2200 punktów Wynik testu należy oświadczyć w formularzu ofertowym Zamawiający zastrzega sobie prawo do wykonania testu PC Mark 10 Digital Content Creation na etapie odbioru na losowo wybranej 10% próbie. Odbiór nastąpi po pozytywnym osiągnięciu wyniku przetestowanego sprzętu
Klawiatura	Klawiatura z wydzieloną strefą numeryczną (układ US), min 98 klawiszy. 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 2x2W Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy Kamera internetowa z diodą informującą o aktywności, trwale zainstalowana w obudowie matrycy. 1 port audio typu combo (słuchawki i mikrofon)
Łączność bezprzewodowa	Wi-Fi 5 AC 201 2x2 + Bluetooth 4.2
Bateria i zasilanie	Bateria umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin Czas pracy na baterii min. 8 godzin Zasilacz o mocy min. 45W
Waga i wymiary	Waga max 1.7 kg z baterią Wysokość laptopa nie większa niż 20mm
Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane, uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią
Certyfikaty	Certyfikat ISO9001, ISO14001, ISO50001 dla producenta sprzętu Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki Potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym
Oprogramowanie antywirusowe	W wyniku rekomendacji z dnia 9 maja 2022 r. wydanej przez Kolegium do Spraw Cyberbezpieczeństwa w sprawie niestosowania w systemach informacyjnych oprogramowania, którego producentem jest Kaspersky Lab z siedzibą w Moskwie (Federacja Rosyjska), na które składa się w szczególności oprogramowanie: Kaspersky Internet Security, Kaspersky Anti-Virus, Kaspersky TOTAL Security oraz Kaspersky Safe Kids, ze względu na stwierdzony negatywny wpływ tego oprogramowania na bezpieczeństwo publiczne nie dopuszcza się stosowania w/w oprogramowania.

	System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej: - wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji - wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych - wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear) Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej. Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach. Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows. Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom. Zarządzanie przez Chmurę: - musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach - musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury - musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur - musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy - musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer Oprogramowanie klienckie, zarządzane z poziomu serwera System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej: - różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie - funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD - funkcje regulowania połączeń WiFi i Bluetooth - funkcje blokowania dostępu dowolnemu urządzeniu - zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu - możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka Monitorowanie zmian w plikach: - możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych - funkcje monitorowania określonych rodzajów plików - możliwość wykluczenia określonych plików/folderów dla procedury monitorowania - generator raportów do funkcjonalności monitora zmian w plikach - możliwość śledzenia zmian we wszystkich plikach - możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach - możliwość definiowana własnych typów plików Optymalizacja systemu operacyjnego stacji klienckich: - usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku - optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem

	- możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich - instruktaż stanowiskowy pracowników Zamawiającego - dokumentacja techniczna w języku polskim Moduł oprogramowania pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa - wymagania dotyczące technologii: - dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową - portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta. - dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych - rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących - nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie Portal zarządzający musi umożliwiać: - przegląd wybranych danych na podstawie konfigurowalnych widgetów - zablokowania możliwości zmiany konfiguracji widgetów - zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów - tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności - eksport wszystkich skanów podatności do pliku CSV Backup i przywracanie danych (licencja wieczysta) - deduplikacja danych - backup przyrostowy i różnicowy - wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji - backup danych lokalnych – plikowy oraz poczty outlook - backup otwartych plików (vss) - filtr plików oraz folderów - domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.), - wyłączanie komputera po wykonaniu backupu - przywracanie danych do wskazanej lokalizacji - możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora - wyszukiwanie plików w repozytorium użytkownika Ustawienia - automatyczne logowanie - zapamiętywanie danych logowania - automatyczne uruchamianie programu przy starcie systemu - ustawianie priorytetu dla procesu backupu - zmiana klucza szyfrującego - ustawienia przepustowości/zajętości pasma - konfiguracja wydajności procesu backupu Bezpieczeństwo - zastępowanie nazwy pliku guid-em - szyfrowanie danych algorytmem aes 256 cbc, zawsze po stronie komputera użytkownika - kompresja danych - transmisja po bezpiecznym protokole tls - deklaracja klucza szyfrującego dane użytkownika - szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji - obliczanie sumy kontrolnej - kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center na terenie Polski. WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 10 i nowsze, Mac OS,Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Wsparcie techniczne, świadczone w języku polskim, zawarte jest w cenie licencji
Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. Pełna funkcjonalność systemu diagnostycznego musi być realizowana bez użycia : dostępu do sieci

	i internetu, dysku twardego również w przypadku jego braku, urządzeń zewnętrznych i wewnętrznych typu : pamięć flash, USBpen itp.
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
System operacyjny	Zainstalowany system operacyjny Windows 10 Professional lub Windows 11 Professional
Porty i złącza	Wbudowane porty i złącza: 1x HDMI 1.4 1x RJ-45, 3x USB Typ-A w tym min. 2x USB 3.2, port zasilania, złącze linki zabezpieczającą

Monitor – 35 szt.

Nazwa	Wymagane parametry techniczne
Typ matrycy	TFT-TN
Przekątna ekranu	Min. 21.5”
Powierzchnia matrycy	Matowa
Rozdzielczość	Min. 1920x1080
Gniazda we/wy	• 1 x 3,5 mm minijack • 1 x 15-pin D-Sub • 1 x HDMI
Wbudowane głośniki	Tak
Ilość kolorów	16,7 mln
Częstotliwość	Min. 75 Hz
Waga	Nie więcej niż 3.6 kg

Microsoft Office 2021 – 39 szt.

Rodzaj	Microsoft Office 2021 Home&Business 2021
Wersja	Box/cyfrowa
Czas trwania	Licencja wieczysta
Wersja językowa	Polska