IZP.271.18.2022

Załącznik nr 2A do SWZ- Opis przedmiotu zamówienia dla części A

Zadanie: Zakup 18 laptopów i 4 komputerów stacjonarnych wraz monitorami w ramach umowy o powierzenia grantu nr 1344/2022 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Wsparcie dzieci z rodzin pegeerowskich w rozwoju cyfrowym – Granty PPGR".

LAPTOP-18 szt.

Procesor	Oferowany komputer przenośny musi osiągać w teście wydajności : PC Mark10 – wynik min. 2600 punktów – test z przeprowadzonej konfiguracji załączyć na wezwanie zamawiającego.
Karta graficzna	Zintegrowana karta graficzna osiągająca w teście SysMark25 Creativity co najmniej 550 punktów.
Pamięć	Zainstalowana pamięć min. 8GB DDR4, z możliwością rozbudowy do min. 16GB RAM.(Nie dopuszcza się wlutowanych pamięci w płytę główną).
Matryca	15,6'' Matowa 1920 x 1080 (FHD 1080), IPS.
Dysk twardy SSD	Pojemność min. 256 GB, interfejs PCI-Express Komputer musi oferować montaż dwóch dysków w konfiguracji M.2+2.5.
Porty Video	1x HDMI
Interfejsy sieciowe	1x 10/100/1000 Mbit/s Wi-Fi 802.11 ac 2x2 Bluetooth 5
Porty USB	3 x USB Type-A w tym min. 2x USB 3.2
Pozostałe porty we/wy	1 x Audio 1 x RJ-45 złącze linki zabezpieczającej.
Kamera internetowa	HD 720p
Dźwięk	Głośniki Stereo 2W x 2 Dolby Audio
Bateria	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
Normy i certyfikaty	Certyfikat ISO9001, ISO14001, ISO50001
Waga	Nie przekraczająca 1,7 kg
System operacyjny – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	Zainstalowany system operacyjny Windows 11, musi umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego, lub równoważny, który spełnia 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 wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6.Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 11. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 12. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 13. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 14. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 15. Umożliwienie zablokowania urządzenia w ramach danego konta. 16. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 17. Zdalna pomoc i współdzielenie aplikacji. 18. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 19. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie

	bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.
Oprogramowanie zabezpieczające – w formularzu oferty należy podać pełną nazwę oferowanego 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: 1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych sieciach 2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury 3. Musi posiadać zdolność do promowania skutecznej polityki w ramach sieci domowej. 4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy 5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania. 1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące komputery, również w sieci domowej. 2. Oprogramowanie klienckie, zarządzane z poziomu serwera. System musi umożliwiać, w sposób centralnie zarządzany z konsoli, 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: 1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową 2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta. 3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych 4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących 5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 6. Portal zarządzający musi umożliwiać: a) przegląd wybranych danych na podstawie konfigurowalnych widgetów b) zablokowania możliwości zmiany konfiguracji widgetów c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności e) eksport wszystkich skanów podatności do pliku CSV Backup i przywracanie danych: a. Deduplikacja danych, b. Backup przyrostowy i różnicowy, c. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, d. Backup danych lokalnych – plikowy oraz poczty Outlook, e. Backup otwartych plików (VSS),

	f. Filtr plików oraz folderów, g. Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.), h. Wyłączanie komputera po wykonaniu backupu, i. Przywracanie danych do wskazanej lokalizacji, j. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora, k. Wyszukiwanie plików w repozytorium użytkownika, l. Automatyczne logowanie, m. Zapamiętywanie danych logowania, n. Automatyczne uruchamianie programu przy starcie systemu, o. Ustawianie priorytetu dla procesu backupu, p. Zmiana klucza szyfrującego, q. Ustawienia przepustowości/zajętości pasma, r. Konfiguracja wydajności procesu backupu, Bezpieczeństwo a. Zastępowanie nazwy pliku GUID-em, b. Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika, c. Kompresja danych, d. Transmisja po bezpiecznym protokole TLS, e. Deklaracja klucza szyfrującego dane użytkownika, f. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, g. 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.
Gwarancja	Minimum 36 miesięczna gwarancja, czas reakcji serwisu, nie później niż w ciągu 3 dni od momentu zgłoszenia usterki.
Uwagi	Komputer fabrycznie nowy

KOMPUTER STACJONARNY- 4 szt.

Procesor	Oferowany komputer przenośny musi osiągać w teście wydajności : PC Mark10 – wynik min. 2600 punktów – test z przeprowadzonej konfiguracji załączyć na wezwanie zamawiającego. 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, 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	Zainstalowana pamięć min. 8GB DDR4, maksymalna dostępna 64GB

Dysk twardy SSD	Pojemność min. 256 GB, interfejs PCI-Express
Porty Video	1xVGA (15 pin D-Sub), 1 x HDMI
Interfejsy sieciowe	1x 10/100/1000 Mbit/s Wi-Fi 802.11a/b/g/n/ac Bluetooth
Napęd optyczny	DVD-RW
Porty USB	2 x USB 2.0 Type-A 2 x USB 3.0 Type-A 2 x USB 3.1 Type-A
Pozostałe porty we/wy	1 x Audio (Mikrofon) 1 x Audio (Line-out) 1 x Audio (Combo) 1 x RJ-45
Gniazda rozszerzeń	1 x PCIe 3.0 x 1 1 x PCIe 3.0 x 16 2 x M.2
Moc zasilacza	Min. 300W 80 PLUS
Kolor	Czarny
Rodzaj obudowy	Tower
Waga	Nie przekraczająca 8,0 kg
System operacyjny – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	Zainstalowany system operacyjny Windows 11, musi umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego, lub równoważny, który spełnia 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 wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6.Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.

	13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta. 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.
Oprogramowanie zabezpieczające – w formularzu oferty należy podać pełną nazwę oferowanego 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: 1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych sieciach 2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury 3. Musi posiadać zdolność do promowania skutecznej polityki w ramach sieci domowej. 4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy 5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania. 1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące komputery, również w sieci domowej. 2. Oprogramowanie klienckie, zarządzane z poziomu serwera. System musi umożliwiać, w sposób centralnie zarządzany z konsoli, 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: 1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową 2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta. 3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych 4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących 5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie 6. Portal zarządzający musi umożliwiać: a) przegląd wybranych danych na podstawie konfigurowalnych widgetów b) zablokowania możliwości zmiany konfiguracji widgetów c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów. d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności e) eksport wszystkich skanów podatności do pliku CSV Backup i przywracanie danych: s. Deduplikacja danych, t. Backup przyrostowy i różnicowy, u. Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, v. Backup danych lokalnych – plikowy oraz poczty Outlook, w. Backup otwartych plików (VSS), x. Filtr plików oraz folderów, y. Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.), z. Wyłączanie komputera po wykonaniu backupu, aa. Przywracanie danych do wskazanej lokalizacji, bb. Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora, cc. Wyszukiwanie plików w repozytorium użytkownika, dd. Automatyczne logowanie, ee. Zapamiętywanie danych logowania, ff. Automatyczne uruchamianie programu przy starcie systemu, gg. Ustawianie priorytetu dla procesu backupu, hh. Zmiana klucza szyfrującego, ii. Ustawienia przepustowości/zajętości pasma, jj. Konfiguracja wydajności procesu backupu, Bezpieczeństwo h. Zastępowanie nazwy pliku GUID-em, i. Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika, j. Kompresja danych,

	k. Transmisja po bezpiecznym protokole TLS, l. Deklaracja klucza szyfrującego dane użytkownika, m. Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, n. 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.
Gwarancja	Minimum 36-miesięczna gwarancja, czas reakcji serwisu, nie później niż w ciągu 3 dni od momentu zgłoszenia usterki.
Uwagi	Komputer fabrycznie nowy

Monitor- 4 szt.

Nazwa komponentu	**Wymagane parametry**
Typ ekranu	Ekran ciekłokrystaliczny o przekątnej min. 21.5
Rozmiar plamki	Max 0,28 mm
Jasność	Min 250 cd/m2
Kontrast	Min. 1000:1
Kąty widzenia (pion/poziom)	Min. 178/178 stopni
Czas reakcji matrycy	max 8 ms
Rozdzielczość maksymalna	Min. 1920 x 1080 przy 60Hz
Pochylenie monitora	W zakresie min/ 25 stopni
Powłoka powierzchni ekranu	Antyodblaskowa
Podświetlenie	System podświetlenia LED
Zużycie energii	maksymalne 40W, czuwanie więcej niż 0,5W
Bezpieczeństwo	Monitor musi być wyposażony w tzw. Kensington Slot
Waga bez podstawy	Maksymalnie 5 kg
Złącze	1x 15-stykowe złącze D-Sub, 1x złącze HDM
Gwarancja	Minimum 36-miesięczna gwarancja, czas reakcji serwisu, nie później niż w ciągu 3 dni od momentu zgłoszenia usterki.
Certyfikaty	CE, ISO9001, ISO 50 001, Energy Star
Inne	Odłączana stopa z VESA. Do monitora powinny być dołączone przewody: display port, VGA.