

Opis Przedmiotu Zamówienia – część numer 1

Dostawa komputerów przenośnych z systemem operacyjnym, oprogramowaniem MS Office i oprogramowaniem antywirusowym

1. Komputer przenośny - laptop (3 sztuki)

Lp.	Nazwa podzespołu, parametru, elementu, lub cechy	Wymagane parametry minimalne
1.	Typ	Komputer przenośny - w ofercie wymagane jest podanie modelu, symbolu oraz producenta.
2.	Ekran	Matryca IPS lub MVA lub EWW (kąty widzenia min. 178 stopni), min. 15,6" z podświetleniem w technologii LED, powłoka antyrefleksyjna Anti-Glare- rozdzielczość: FHD 1920x1080. Ekran umożliwiający pracę w 4 trybach, w tym z niską emisją niebieskiego światła.
3.	Wydajność komputera	Oferowany komputer przenośny musi osiągać w teście wydajności: SYSMARK 25 - wynik min. 1100 - test z przeprowadzonej konfiguracji 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 urządzeniach. Nie dopuszcza się stosowania overclockingu, 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.
4.	Procesor	Procesor wielordzeniowy, osiągający w teście PassMark CPU Mark wynik min. 13000 pkt według wyników ze strony https://www.cpubenchmark.net/cpu_list.php
5.	Płyta główna	Wyposażona w dedykowany chipset dla oferowanego procesora. Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejs SATA III (6 Gb/s) do obsługi dysków twardej. Płyta główna i konstrukcja laptopa wspierająca konfigurację dwu dyskową SSD M.2+M.2.
6.	Pamięć RAM	Min. 16GB DDR4 2400Mhz z możliwością rozbudowy do min. 32GB. Dwa wymienne złącza pamięci.
7.	Pamięć masowa	Min. 512GB SSD M.2 PCIe Możliwość rozbudowy o drugi dysk twardej M.2.

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

8.	Karta graficzna	Karta graficzna ze sprzętowym wsparciem dla DirectX 12, obsługiwana rozdzielczość 4K poprzez port HDMI min. 4096x2304@24Hz. Pamięć do 2GB RAM. Osiągająca w teście Passmark Average G3D Mark min. 1500 pkt.
9.	Klawiatura i touchpad	Klawiatura podświetlana z powłoką antybakteryjną, odporna na zalanie cieczą. Klawiatura w układzie US-QWERTY z klawiaturą numeryczną. Touchpad wyposażony w 2 niezależne klawisze funkcyjne ze wsparciem dla technologii multitouch. Musi posiadać wsparcie dla gestów dla minimum 3 niezależnych punktów dotyku.
10.	Multimedia	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wbudowane głośniki stereo o mocy 2W. Mikrofon z funkcją redukcji szumów i poprawy mowy wbudowane w obudowę matrycy. Kamera internetowa 720p trwale zainstalowana w obudowie matrycy wraz z diodą LED sygnalizującą pracę kamery.
11.	Bateria i zasilanie	Min. 4-komorowa, min. 3400mAh pozwalająca na nieprzerwaną pracę przez min. 6 godzin wg oficjalnych dokumentów producenta. Umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin. Zasilacz o mocy min. 65W. 2 lata gwarancji na baterię.
12.	Waga i wymiary	Waga maksymalnie 2,0 kg z baterią.
13.	Obudowa	Szkielet, zawiasy oraz krawędzie matrycy laptopa wykonane ze wzmocnianego aluminium. Obudowa wyposażona w zawiasy metalowe. W obudowę wbudowane co najmniej 2 diody sygnalizujące stan naładowania akumulatora oraz pracę dysku twardego.
14.	BIOS	Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: <ul style="list-style-type: none"> – Wersji BIOS wraz z bieżącą datą, – Numerze seryjnym komputera, – Ilości pamięci RAM, – Modelu procesora oraz częstotliwości jego taktowania, – Modelu dysku twardego wraz z jego numerem seryjnym, – Możliwość wyłączenia karty LAN, – Możliwość wyłączenia karty WLAN, – Możliwość wyłączenia zintegrowanej karty AUDIO, – Możliwość wyłączenia czytnika kart, – Możliwość wyłączenia portów USB. <p>Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.</p> <p>Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z USB.</p> <p>Możliwość, bez uruchamiania systemu operacyjnego, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora. Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora, a hasłem systemowym tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe.</p>
15.	Certyfikaty	Certyfikat ISO9001, ISO14001, ISO 50001 dla producenta komputera.

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		Deklaracja zgodności CE (dostarczyć na wezwanie Zamawiającego). Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki - (dostarczyć na wezwanie Zamawiającego).
16.	Bezpieczeństwo	Zintegrowany z chipsetem płyty głównej 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 (TPM 2.0). Czujnik spadania zwiększający ochronę dysków twardej działający nawet przy wyłączonym notebooku oraz konstrukcja absorbująca wstrząsy. Złącze typu Kensington Lock/Noble Lock. Czytnik linii papilarnych.
17.	System operacyjny – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	Windows 11 Professional 64 bity PL. Dołączony zewnętrzny nośnik lub partycja Recovery umożliwiająca w przypadku awarii dysku twardego ponowną instalację zainstalowanego systemu operacyjnego oraz nośnik zawierający sterowniki wszystkich zainstalowanych urządzeń.
18.	Dodatkowe oprogramowanie – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	Oprogramowanie zarządzające producenta komputera, instalowane na etapie produkcji komputera, umożliwiające min.: - monitorowanie komputera i generowanie zgłoszeń o błędach / nieprawidłowym działaniu w zakresie pracy komponentów i wydajności systemów, - powiadamiania o nowych wersjach sterowników i umożliwienie użytkownikowi wykonania upgrade systemu, - powiadamianie o problemach wydajnościowych i diagnozowanie / rozwiązywanie takich problemów, - śledzenia kluczowych komponentów i przewidywanie awarii przed ich wystąpieniem. Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające: - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, - możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem, a w szczególności informacji o: <ul style="list-style-type: none"> • poprawkach i usprawnieniach dotyczących aktualizacji, • dacie wydania ostatniej aktualizacji, • priorytecie aktualizacji, • zgodności z systemami operacyjnymi, • jakiego komponentu sprzętu dotyczy aktualizacja, • wszystkich poprzednich aktualizacjach z informacjami jak powyżej, • wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne. - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga, - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr), - sprawdzenia historii upgrade'u z informacją, jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania), - dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością eksportu do pliku o rozszerzeniu *.xml, - raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiorem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość eksportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.
19.	Porty i złącza	Porty i złącza: 1x HDMI ver. 1.4 3x USB 3.2 w tym min. 1x USB 3.1 typ-C (z Displayport). Możliwość ładowania urządzeń zewnętrznych poprzez port USB, nawet gdy notebook jest wyłączony i jest w trybie hibernacji/uśpienia. Czytnik kart multimedialnych 4w1 wspierający karty SD 4.0. Wbudowana karta LAN 10/100/1000 Mbps RJ45. Współdzielone złącze słuchawkowe stereo i złącze mikrofonowe tzw. combo. Moduł bluetooth 5.0 Zintegrowana w postaci wewnętrznego modułu mini-PCI Express karta sieci WLAN 5 obsługująca łącznie standardy IEEE 802.11 a/b/g/n w standardzie AC.
20.	Warunki gwarancji	Minimum 24 miesiące gwarancji. Czas reakcji serwisu - do końca następnego dnia roboczego. Firma serwisująca musi posiadać ISO 9001:2000 lub równoważny certyfikat dla świadczenia usług serwisowych oraz posiadać autoryzację producenta komputera - dokumenty potwierdzające dostarczyć na wezwanie Zamawiającego. Gwarancja musi oferować przez cały okres: dostępność wsparcia technicznego przez 24 godziny 7 dni w tygodniu przez cały rok. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta notebooka realizowany poprzez podanie na dedykowanej stronie internetowej producenta nazwy platformy notebooka.
21.	Pakiet biurowy	Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej. 2. Wymagania odnośnie interfejsu użytkownika: a) pełna polska wersja językowa interfejsu użytkownika, b) prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. 3. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: a) posiada kompletny i publicznie dostępny opis formatu, b) ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, c) pozwala zapisywać dokumenty w formacie XML. 4. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb Zamawiającego. 5. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

	<p>i aplikacjami (język makropoleceń, język skryptowy).</p> <p>6. Do aplikacji pakietu musi być dostępna pełna dokumentacja w języku polskim.</p> <p>7. Pakiet zintegrowanych aplikacji biurowych musi zawierać:</p> <ol style="list-style-type: none">Edytor tekstów.Arkusze kalkulacyjny.Narzędzie do przygotowywania i prowadzenia prezentacji.Narzędzie do zarządzania informacją prywatną (poczta elektroniczna, kalendarzem, kontaktami i zadaniami). <p>8. Edytor tekstów musi umożliwiać:</p> <ol style="list-style-type: none">Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.Wstawianie oraz formatowanie tabel.Wstawianie oraz formatowanie obiektów graficznych.Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.Automatyczne tworzenie spisów treści.Formatowanie nagłówek i stopek stron.Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.Określenie układu strony (pionowa/pozioma), niezależnie dla każdej sekcji dokumentu.Wydruk dokumentów.Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007 lub Microsoft Word 2010, 2013, 2016 i 2019 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.Wymagana jest dostępność mechanizmów umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa. <p>9. Arkusz kalkulacyjny musi umożliwiać:</p> <ol style="list-style-type: none">Tworzenie raportów tabelarycznych.Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze
--	--

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		<p>kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML).</p> <ul style="list-style-type: none">e) Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych.f) Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.g) Wyszukiwanie i zamianę danych.h) Wykonywanie analiz danych przy użyciu formatowania warunkowego.i) Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.j) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.k) Formatowanie czasu, daty i wartości finansowych z polskim formatem.l) Zapis wielu arkuszy kalkulacyjnych w jednym pliku.m) Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 oraz Microsoft Excel 2010, 2013, 2016 i 2019, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.n) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. <p>10. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:</p> <ul style="list-style-type: none">a) Przygotowywanie prezentacji multimedialnych.b) Prezentowanie przy użyciu projektora multimedialnego.c) Drukowanie w formacie umożliwiającym robienie notatek.d) Zapisanie jako prezentacja tylko do odczytu.e) Nagrywanie narracji i dołączanie jej do prezentacji.f) Opatrywanie slajdów notatkami dla prezentera.g) Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.h) Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.i) Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.j) Możliwość tworzenia animacji obiektów i całych slajdów.k) Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.l) Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2007, MS PowerPoint 2010, 2013, 2016 i 2019. <p>11. Narzędzie do zarządzania informacją prywatną (poczta elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:</p> <ul style="list-style-type: none">a) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.b) Przechowywanie wiadomości na serwerze lub w lokalnym pliku stworzonym z zastosowaniem efektywnej kompresji danych.c) Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.d) Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną.e) Automatyczne grupowanie wiadomości poczty o tym samym tytule.f) Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.
--	--	---

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		<p>g) Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.</p> <p>h) Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.</p> <p>i) Zarządzanie kalendarzem.</p> <p>j) Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.</p> <p>k) Przeglądanie kalendarza innych użytkowników.</p> <p>l) Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.</p> <p>m) Zarządzanie listą zadań.</p> <p>n) Zlecanie zadań innym użytkownikom.</p> <p>o) Zarządzanie listą kontaktów.</p> <p>p) Udostępnianie listy kontaktów innym użytkownikom.</p> <p>q) Przeglądanie listy kontaktów innych użytkowników.</p> <p>r) Możliwość przesyłania kontaktów innym użytkownikom.</p> <p>s) Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.</p>
--	--	--

2. Oprogramowanie zabezpieczające - antywirus (3 sztuki)

Lp.	Element konfiguracji	Wymagane parametry minimalne
1.	Bezpieczeństwo i oprogramowanie dodatkowe – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	<p>System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej:</p> <ul style="list-style-type: none"> wykrywanie i blokowanie plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają w czasie rzeczywistym algorytmów kompresji, wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych, stosowanie kwarantanny, wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear), skanowanie urządzeń USB natychmiast po podłączeniu, automatyczne odłączanie zainfekowanej końcówki od sieci, skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji. <p>Zarządzanie „aktywami” stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontaktach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach.</p>

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		<p>Musi posiadać moduł ochrony IDS/IPS Musi posiadać mechanizm wykrywania skanowania portów Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości</p> <p>Szyfrowanie danych:</p> <ul style="list-style-type: none">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. <p>Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej. Istnieje możliwość blokady zapisywania 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. Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware. Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające i zapobiegające prze niezamierzonymi manipulacjami - ataki ransomware. Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:</p> <ul style="list-style-type: none">przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli,zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory,tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux,centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.raportowanie dostępne przez dedykowany panel w konsoli,
--	--	---

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		<p>z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich,</p> <ul style="list-style-type: none">definiowanie struktury, zarządzanie oparte o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji. <p>Zarządzanie przez Chmurę:</p> <ol style="list-style-type: none">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.Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń.Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej. <p>Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralne zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.</p> <p>Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.</p> <ol style="list-style-type: none">Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer.Oprogramowanie klienckie, zarządzane z poziomu serwera. <p>System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:</p> <ul style="list-style-type: none">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 kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe,funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi,funkcje blokowania dostępu dowolnemu urządzeniu,możliwość tymczasowego dodania dostępu do urządzenia przez administratora,zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu,możliwość zablokowania funkcjonalności portów USB, blokując dostęp
--	--	---

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		<p>urządzeniom innym niż klawiatura i myszka,</p> <ul style="list-style-type: none">• możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora,• możliwość zarządzania urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry,• możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich,• funkcję wirtualnej klawiatury.• możliwość blokowania każdej aplikacji,• możliwość zablokowania aplikacji w oparciu o kategorie,• możliwość dodania własnych aplikacji do listy zablokowanych,• zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjną na serwerze,• dodawanie innych aplikacji,• dodawanie aplikacji w formie portable,• możliwość wyboru pojedynczej aplikacji w konkretnej wersji,• dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB,• kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool,• możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki,• możliwość zablokowania funkcji Printscreen,• funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx,• funkcje monitorowania i kontroli przepływu poufnych informacji,• możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukiwania w różnych typach plików,• możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj,• możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe,• ochronę przed wyciekami informacji na drukarki lokalne i sieciowe,• ochrona zawartości schowka systemu,• ochrona przed wyciekami informacji w poczcie e-mail w komunikacji SSL,• możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych,• ochrona plików zamkniętych w archiwach,• zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekami,• możliwość tworzenia profilu DLP dla każdej polityki,• wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania,• ochrona przed wyciekami plików poprzez programy typu p2p <p>Monitorowanie zmian w plikach:</p> <ul style="list-style-type: none">• możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych,• funkcje monitorowania określonych rodzajów plików,
--	--	--

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		<ul style="list-style-type: none">• 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. <p>Optymalizacja systemu operacyjnego stacji klienckich:</p> <ul style="list-style-type: none">• usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku,• optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem,• możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich,• instruktaż stanowiskowy pracowników Zamawiającego,• dokumentacja techniczna w języku polskim. <p>Wspierane platformy i systemy operacyjne:</p> <ol style="list-style-type: none">1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)3. Mac OS X, Mac OS 104. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat <p>Platforma do zarządzania dla Android i iOS:</p> <p>Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS, a także ich ochronę.</p> <p>Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.</p> <p>Zarządzanie użytkownikiem.</p> <p>Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email.</p> <p>Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika.</p> <p>Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi.</p> <p>Musi posiadać możliwość eksportu danych użytkownika.</p> <p>Zarządzanie urządzeniem.</p> <p>Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO.</p> <p>Musi umożliwiać import listy urządzeń z pliku CSV.</p> <p>Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych.</p> <p>Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta.</p> <p>Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał.</p>
--	--	---

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

		<p>Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres.</p> <p>Musi zawierać podgląd aktualnie zainstalowanych aplikacji.</p> <p>Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych,</p> <p>Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł.</p> <p>Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres</p> <p>Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa.</p> <p>Wymagania dotyczące technologii:</p> <p>Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową.</p> <p>Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.</p> <p>Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:</p> <ul style="list-style-type: none"> - Microsoft Internet Explorer - Microsoft Edge - Mozilla Firefox - Google Chrome - Safari <p>Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących.</p> <p>Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie.</p> <p>Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:</p> <ul style="list-style-type: none"> - Windows 2008 R2 - Windows 2012 - Windows 2012 R2 - Windows 2016 <p>Portal zarządzający musi umożliwiać:</p> <ol style="list-style-type: none"> 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.
2.	Wymagania dodatkowe	Dołączone oprogramowanie w momencie dostawy musi być zainstalowane na wszystkich dostarczonych laptopach (3 sztuki). Długość licencji minimum 24 miesiące.