Załącznik - Nr 1

Komputer stacjonarny – Ilość 12 szt.

Typ parametru	Wymaganie
Komputer stacjonarny	Komputer stacjonarny będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do zasobów lokalnej sieci komputerowej oraz usług sieci Internet, aplikacji graficznych wektorowych oraz rastrowych, a także danych multimedialnych.
Obudowa	Typu SFF z obsługą kart PCI Express wyłącznie o niskim profilu: - 1 x PCI Express 4.0 x16, - 2 x PCI Express 3.0 x1 Wyposażona w min. 3 kieszenie z czego min. 1 szt. 5,25” (dopuszcza się zastosowanie jednej kieszeni 5,25” w wersji SLIM dla napędu optycznego) Obudowa umożliwiająca montaż 3 dysków, w tym minimum 1 na złączu M.2 PCIe NVME. Obudowa musi umożliwiać bez narzędziowe otwarcie, demontaż dysków twardych (3,5” oraz 2,5”), napędu optycznego oraz kart rozszerzeń. Obudowa musi być wyposażona w czujnik otwarcia. Wbudowany głośnik o mocy 1W Obudowa trwale oznaczona nazwą producenta, nazwą komputera, PN, numerem seryjnym
Chipset	Dostosowany do zaoferowanego procesora
Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera.
Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych klasy x86. Punktacja procesora na poziomie wydajności liczonej w punktach równa lub wyższa procesorowi Intel® Core™ i5-12400 na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na **http://www.cpubenchmark.net/**. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
Pamięć operacyjna	Min 16 GB z możliwością rozbudowy do 128GB.
Dysk twardy	512GB SSD M.2 PCIE NVME, wspierający sprzętowe szyfrowanie dysku, zawierający RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
Napęd optyczny	Wbudowana w obudowę komputera nagrywarka DVD-RW.
Karta graficzna	Zintegrowania karta graficzna.
Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.
Sieć	10/100/1000 – złącze RJ45 Wbudowana bezprzewodowa karta sieciowa wifi AC min. 2x2 Bluetooth min. 5.1
Porty/złącza	Wbudowane porty: - 1 x HDMI, - 2 x DP, - co najmniej 8 x USB w tym: min 2 - 4 x USB 3.2 z przodu obudowy i min 2 - 4 x USB 2.0 z tyłu obudowy; jedno z w.w złącz musi być w standardzie USB typ C - port sieciowy RJ-45, - porty słuchawek i mikrofonu na przednim panelu obudowy oraz z tyłu obudowy (dopuszcza się rozwiązanie typu combo) - czytnik kart pamięci SD lub microSD Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
Klawiatura/mysz	Zestaw: Klawiatura USB w układzie US z kablem o długości min. 1,8 m.+ Mysz optyczna USB z klawiszami oraz rolką (scroll) z kablem o długości min. 1,8 m.
Zasilacz	Energooszczędny zasilacz o mocy nie większej niż 280W oraz sprawności na poziomie min. 80%

Załącznik - Nr 1

BIOS	BIOS zgodny ze specyfikacją UEFI - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: - modelu komputera, PN - numerze seryjnym, - numerze inwentarzowym (AssetTag), - MAC Adres karty sieciowej, - wersja Biosu wraz z datą produkcji, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem, - stanie pracy wentylatora na procesorze - stanie pracy wentylatora w obudowie komputera - napędach lub dyskach podłączonych do portów SATA (model dysku twardego i napędu optycznego)Możliwość z poziomu Bios: - wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy - wyłączenia selektywnego (pojedynczego) portów SATA, - wyłączenia karty sieciowej, karty audio, portu szeregowego, - możliwość ustawienia portów USB w jednym z dwóch trybów: 1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej - ustawienia hasła: administratora, Power-On, HDD, - blokady aktualizacji BIOS bez podania hasła administratora - wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów - alertowania zmiany konfiguracji sprzętowej komputera - wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan) - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - załadowania optymalnych ustawień Bios - obsługa Bios za pomocą klawiatury i myszy
Certyfikaty i standardy	1. Producent komputera musi posiadać ISO 9001. 2. Producent komputera musi posiadać ISO14001. 4. Producent komputera musi posiadać TCO min. 9.0. 5. Oferowane komputery stacjonarne muszą posiadać europejską deklaracja zgodności CE. 6. Producent komputera musi posiadać potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych.
Bezpieczeństwo	1. Złącze typu Kensington Lock 2. Oczko na kłódkę 3. Moduł dTPM 2.0
System operacyjny	Zainstalowany system operacyjny co najmniej Windows 11 Pro 64-bitowy w polskiej wersji językowej lub system równoważny. Klucz licencyjny systemu musi być zapisany trwale w BIOS i umożliwiać jego instalację bez potrzeby ręcznego wpisywania klucza licencyjnego. **Zamawiający nie dopuszcza zaoferowania systemu operacyjnego pochodzącego z rynku wtórnego, reaktywowanego systemu.** System równoważny 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 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

Załącznik - Nr 1

	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 tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 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 – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 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. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 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. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
Gwarancja	36 miesięcy świadczona w miejscu użytkowania sprzętu (on-site) W przypadku awarii dysków twardych, dysk pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
Wsparcie techniczne producenta	- możliwość weryfikacji u producenta konfiguracji fabrycznej zakupionego sprzętu. - możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji. - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego.

Załącznik - Nr 1

Monitor – 12 sztuk

Typ parametru	Wymaganie
Monitor	Monitor będzie wykorzystywany dla potrzeb aplikacji biurowych, obróbki zdjęć lub wideo.
Proporcje obrazu	16:9
Przekątna ekranu	Min. 23,8”
Typ matrycy	Typu IPS/PLS/MVA/WVA o wykończeniu matowym (nie dopuszcza się naklejek matowiących matrycę)
Technologia podświetlania	Diody LED
Obszar widzialny w pionie	Min. 296,46 mm
Obszar widzialny w poziomie	Min. 527 mm
Plamka matrycy	nie większy niż – 0.312 mm
Rozdzielczość	Rozdzielczość nie mniejsza niż: FHD (1920x1080)
Czas reakcji	min. 6 ms
Jasność	Jasność nie mniejsza niż 250 cd/m2
Kontrast statyczny	1000:1
Kąt widzenia poziomy	min. 170 °
Kąt widzenia pionowy	min. 170 °
Porty/złącza	Minimalna ilość dostępnych złącz monitora: - 1x DP - 1x HDMI - 1x VGA - Min. 4x USB 3.1 - 1x audio
Akcesoria w zestawie	Do monitora producent dołącza minimum kable: - HDMI min.1,5m. - Kabel zasilający min.1,5m. - DisplayPort min.1,5m.
Stopa/Podstawa monitora	Musi umożliwiać: - przechylenie w pionie min. 25 stopni (-5 / 20) - Obrót monitora na boki min 45 stopni - Pivot - regulację wysokości min. 15cm
Obudowa	- Musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona). - Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA (100x100). - Wbudowane w obudowę przyciski umożliwiające włączenie, wyłączenie oraz zmianę ustawień wyświetlania monitora. - Obudowa trwale oznaczona nazwą producenta, numerem seryjnym i katalogowym pozwalającym na jednoznaczna identyfikacje zaoferowanego monitora. - Wbudowany zasilacz w obudowie.
Certyfikaty	- Certyfikat EPEAT na poziomie co najmniej Silver. - TCO 8.0 lub wyższy - Energy Star -Redukcja migotania (Flicker free) -Redukcja niebieskiego światła
Kolor	Czarny

Gwarancja	Min. 24 miesiące.

Oprogramowanie Biurowe – 28 sztuk

Typ parametru	Wymaganie
Oprogramowanie biurowe	-Licencja na oprogramowanie typu Microsoft Office 2021 Home & Business PL 32/64 lub równoważne spełniające wymagania równoważności opisane poniżej. -Licencja powinna uprawniać do używania ww. oprogramowania przez Zamawiającego w ramach jego działalności. -Licencja ma być udzielona na czas nieokreślony, bez ograniczeń terytorialnych na polach eksploatacji obejmujących, co najmniej: a) instalację i użytkowanie ww. oprogramowania w pełnej funkcjonalności na dostarczonym Sprzęcie w konfiguracji przedstawionej w ofercie jak i też powstałej w wyniku rozbudowy, w tym poprzez pracowników Zamawiającego, b) sporządzenie jednej kopii zapasowej nośnika, na którym Zamawiający przechowuje zbiory instalacyjne ww. oprogramowania, c) nieodpłatnego pobierania, instalowania i użytkowania poprawek i aktualizacji wydanych dla ww. oprogramowania przez producenta oprogramowania, Licencja powinna umożliwiać: a) instalację ww. oprogramowania na dowolnym komputerze, b) przenoszenie ww. oprogramowania pomiędzy komputerami (po co najmniej 90 dniach pracy). -Wykonawca, który zaoferuje rozwiązanie równoważne, zobligowany jest zawrzeć w ofercie opis oprogramowania równoważnego, zawierający opis parametrów i funkcjonalności dla oprogramowania równoważnego, określonych powyżej. Z opisu powinno jednoznaczne wynikać, że produkt oferowany jako równoważny spełnia wymagania określone przez Zamawiającego. Zastosowanie rozwiązania równoważnego nie będzie wymagało żadnych nakładów po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury. Wszelkie niezbędne prace adaptacyjne (jeśli wystąpi potrzeba ich wykonania), zostaną zrealizowane przez Wykonawcę. Wykonawca dostarczy dokumentację przeprowadzonych prac adaptacyjnych. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie poprawnie współpracować ze sprzętem i oprogramowaniem eksploatowanym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu infrastruktury u Zamawiającego, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania infrastruktury, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu oprogramowania. -Zamawiający wymaga by legalność dostarczanego oprogramowania była wykazana odpowiednimi atrybutami legalności na przykład z tzw. naklejkami GML (Genuine Microsoft Label) lub naklejkami COA (Certificate of Authenticity) stosowanymi przez producenta sprzętu. To można usnąć -Zamawiający w momencie odbioru Sprzętu i oprogramowania przewiduje możliwość zastosowanie procedury sprawdzającej legalność dostarczonego oprogramowania. -Zamawiający dopuszcza możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów komputerowych u Producenta oprogramowania w przypadku wystąpienia wątpliwości co do jego legalności. To bym zostawił daje możliwość weryfikacji jeśli byłyby wątpliwości co do legalności oprogramowania.
	Opis równoważności dla oprogramowania MS Office 2021 Home & Business 32/64 bit PL: 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. Licencja wieczysta 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 r. 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 i aplikacjami (język makropoleceń, język skryptowy). 6. Do aplikacji pakietu musi być dostępna pełna dokumentacja w języku polskim. 7. Pakiet zintegrowanych aplikacji biurowych musi zawierać: a. Edytor tekstów. b. Arkusz kalkulacyjny. c. Narzędzie do przygotowywania i prowadzenia prezentacji. d. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami). 8. Edytor tekstów musi umożliwiać: a. 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. b. Wstawianie oraz formatowanie tabel. c. Wstawianie oraz formatowanie obiektów graficznych.

	d. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). e. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. f. Automatyczne tworzenie spisów treści. g. Formatowanie nagłówków i stopek stron. h. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie. i. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. j. Określenie układu strony (pionowa/pozioma), niezależnie dla każdej sekcji dokumentu. k. Wydruk dokumentów. l. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. m. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007 lub Microsoft Word 2010, 2013, 2016 i 2019,2021 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu. n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. o. Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem. p. Wymagana jest dostępność mechanizmów umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa. 9. Arkusz kalkulacyjny musi umożliwiać: a. Tworzenie raportów tabelarycznych. b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych. c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML). 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 2019,2021, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń. n. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. 10. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać: a. Przygotowywanie prezentacji multimedialnych, które będą: 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 2019,2021. 11. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać: a. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego. b. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym 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. g. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów. h. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie. i. Zarządzanie kalendarzem. j. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników. k. Przeglądanie kalendarza innych użytkowników.

	l. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach. m. Zarządzanie listą zadań. n. Zlecanie zadań innym użytkownikom. o. Zarządzanie listą kontaktów. p. Udostępnianie listy kontaktów innym użytkownikom. q. Przeglądanie listy kontaktów innych użytkowników. r. Możliwość przesyłania kontaktów innym użytkowników. s. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

Laptop – Ilość 2 sztuki

Typ parametru	Wymaganie
Komputer przenośny (laptop)	Komputer przenośny – laptop
Ekran	Matowy, matryca TFT 15.6” z podświetleniem w technologii LED, rozdzielczość FHD 1920x1080, 300 nits, kontrast 800:1 w technologii IPS lub PLS lub WVA Kąt otwarcia pokrywy ekranu min.180 stopni.
Obudowa	Wykonana według normy MIL-STD-810H lub normy równoważnej.
Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera.
Chipset	Dostosowany do zaoferowanego procesora.
Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86. Punktacja procesora na poziomie wydajności liczonej w punktach równa lub wyższa procesorowi Intel® Core™ i5-1235U na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/.
Pamięć operacyjna	Min. 16 GB, pamięć działająca w trybie dual-channel Możliwość rozbudowy pamięci RAM do 40GB.
Dysk twardy	Min. 512GB M.2 SSD PCIe, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. Możliwość rozbudowy do konfiguracji dwudyskowej
Karta graficzna	Dedykowana karta graficzna z m.in. 2GB pamięci własnej.
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki stereo (2x2W), port słuchawek i mikrofonu typu COMBO, kamera video 1080p z mechaniczną zasłoną obiektywu, dwa mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute).
Porty/złącza	Min. porty 3x USB z czego min. dwa porty USB 3.2 z czego jeden port musi umożliwiać ładowanie komputera i transmisję obrazu oraz podłączenie stacji dokującej, złącze słuchawek i złącze mikrofonu typu COMBO, HDMI obsługujący rozdzielczość 4K podłączonego monitora. Złącze umożliwiające podpięcie linki antykradzieżowej. Jeden z portów USB musi obsługiwać Thunderbolt 4. W celu zaoferowania większej liczby portów USB-C wymaga się, aby minimum dwa porty USB były typu A.
Klawiatura	Klawiatura odporna na zalanie cieczą, układ US, klawiatura wyposażona w podświetlanie przycisków.
Czytnik linii papilarnych	Wbudowany czytnik linii papilarnych
Bluetooth	Wbudowany moduł Bluetooth min. 4.1
Karta sieciowa LAN	10/100/1000 wspierająca WOL oraz PXE Boot
Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie AX + Bluetooth

Załącznik - Nr 1

Bateria	Pozwalająca na nieprzerwaną pracę urządzenia do 10 godzin. Ponadto komputer ma być wyposażony w system szybkiego ładowania akumulatora, który umożliwia szybkie naładowanie akumulatora notebooka w czasie 60 minut od 0% do 80%.
Zasilacz	Zasilacz zewnętrzny 65W
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy (przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury). Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - wersji BIOS wraz z datą produkcji BIOS - nr seryjnym komputera - Ilości zainstalowanej pamięci RAM oraz możliwość odczytania informacji o obłożeniu, szybkości i rodzaju z poziomu BIOS lub w zaimplementowanym systemie diagnostycznym - typie procesora i jego prędkości - MAC adresu zintegrowanej karty sieciowej - nr inwentarzowym (tzw. Asset Tag) - wymagane wolne pole do edycji przez administratora - nr seryjnym płyty głównej komputera - informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - Możliwość Wyłączania/Włączania technologii antykradzieżowej - Możliwość ustawienia hasła Administratora - Możliwość ustawienia hasła na zainstalowanym dysku SSD/HDD - Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password - Możliwość przeglądania ustawień BIOS z poziomu użytkownika bez możliwości zmiany ustawień BIOS - Możliwość zabezpieczenia hasłem aktualizacji BIOS - Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS - Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. - Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, karty WiFi, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, portów USB, bluetooth - Możliwość włączenia/wyłączenia funkcji klonowania adresu MAC dla stacji dokującej - Możliwość niezależnego włączenia/wyłączenia płytki dotykowej oraz manipulatora (joysticka) - Funkcja bezpiecznego usuwania danych z dysku dostępna z poziomu BIOS
Certyfikaty i standardy	1. Producent laptopa musi posiadać: - ISO 9001:2000 - ISO 14001 - ISO 50001 2. Energy Star 3. TCO lub TCO Edge 4. Deklaracja zgodności CE
Waga	Waga urządzenia z baterią podstawową max 1.8 kg
Szyfrowanie	Komputer wyposażony w moduł TPM 2.0
System operacyjny	Microsoft Windows 11 Pro 64 bit lub system operacyjny klasy PC, 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.

Załącznik - Nr 1

	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 tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 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 – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 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. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 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. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
Gwarancja	Minimum 24 miesiące on-site (Wyjęcie dysku z komputera nie może być powodem utraty gwarancji). Zamawiający wymaga aby w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostał u Zamawiającego. Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje

	producenta urządzeń. Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
Wsparcie techniczne producenta	- możliwość weryfikacji u producenta konfiguracji fabrycznej zakupionego sprzętu. - możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji. - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego.

Zasilacz UPS – ilość 60 sztuk

Typ parametru	Wymaganie
Minimalne wymagania techniczne dla jednostki UPS	• Moc znamionowa jednostki nie mniej niż 900VA / 540W • Technologia Line Interactive • Temperatura eksploatacji 0 - 40 °C • 10 ms typowo : 12 ms maksymalnie
Parametry wejściowe	• Nominalne napięcie wejściowe 230VAC • Częstotliwość wejściowa 50/60 Hz +/-3 Hz (automatyczne wykrywanie) • Typ gniazda wejściowego Schuko • zakres napięcia wejściowego 170 - 280 VAC
Parametry wyjściowe	Napięcie wyjściowe 230VAC • Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz ±1 Hz • Typ przebiegu schodkowa aproksymacja sinusiody • Złącza/gniazda wyjściowe min 2- PN-E-93201
Akumulatory i czas podtrzymania	• Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy • Typowy czas ładowania ≤12 godziny
Komunikacja i zarządzanie	• USB • Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD • Alarm dźwiękowy Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia • Wyświetlacz LCD musi sygnalizować obsłudze stany ostrzegawcze
Certyfikaty, zgodności oraz gwarancja	Normy: Bezpieczeństwo IEC EN 2040-1: EMC IEC EN 62040-2 C2 lub równoważne Min 24 miesięcy gwarancji naprawy lub wymiany (bez akumulatora) i 12 miesięcy na akumulatory.

Zakup oprogramowania do bezpiecznego pobierania plików – Ilość 85 sztuk

Typ parametru	Wymaganie
Oprogramowania do bezpiecznego pobierania plików	Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe). Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.

	Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami. WYMAGANIA OCHRONA STACJI ROBOCZYCH Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). Rozwiązanie musi wspierać architekturę ARM64. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. "Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach." Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego MS Outlook. "Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: • tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, • tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, • tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, • tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu." Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. WYMAGANIA OCHRONA SERWERA

Załącznik - Nr 1

	Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. Dodatkowe wymagania dla ochrony serwerów Windows: Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. "Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych." Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. Dodatkowe wymagania dla ochrony serwerów Linux: Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. WYMAGANIA SZYFROWANIE System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. WYMAGANIA ENDPOINT DETECTION AND RESPONSE Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS współpracujący z systemem do ochrony stacji roboczych tego samego producenta. Rozwiązanie musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta. Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. Rozwiązanie musi zapewniać wykluczenia dotyczące procesu lub procesu „rodzica". Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia. Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne, pobrania do analizy oraz ich zablokowania. Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł. Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli. Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania poleceń powershell. WYMAGANIA OCHRONA URZĄDZEŃ MOBILNYCH OPARTYCH O SYSTEM ANDROID Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.

Załącznik - Nr 1

	Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. "Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: a. nazwę aplikacji, b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła." **Urząd Gminy Luzino posiada licencje ESET PROTECT Entry ON-PREM w ilości 85 stanowisk. Zamawiając dopuszcza upgrade posiadanych przez zamawiającego licencji.** **Okres trwania licencji: 24 miesiące.**

Oprogramowania do szyfrowania dysków w laptopach – Ilość 25 sztuk

Typ parametru	Wymaganie
Oprogramowania do szyfrowania dysków w laptopach	Konsola centralnego zarządzania musi wspierać systemy operacyjne Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022 oraz Microsoft Windows 7/8/10/11. Serwer centralnego zarządzania musi współpracować co najmniej z silnikami baz danych takimi jak Microsoft SQL Server 2012, 2014, 2016, 2017, 2019 w wersji przynajmniej Express. Konsola centralnego zarządzania musi pozwalać na generowanie pakietów instalacyjnych dla stacji końcowych w formacie MSI. Komunikacja pomiędzy serwerem centralnego zarządzania, a serwerem proxy musi odbywać się na bezpiecznym porcie 443. Administrator musi mieć możliwość tworzenia i zarządzania wieloma kluczami szyfrującymi, opartymi o kilka algorytmów szyfrujących, co najmniej AES, 3DES, Blowfish. Administrator musi mieć możliwość tworzenia różnych użytkowników, mających dostęp do konsoli centralnego zarządzania wraz z możliwością przypisywania im różnych ról. Administrator musi mieć możliwość tworzenia dodatkowych ról, na podstawie opcji dostępnych w konsoli centralnego zarządzania. Logowanie do konsoli centralnego zarządzania powinno być objęte warunkami złożoności hasła. "Musi istnieć możliwość konfiguracji złożoności hasła do konsoli centralnego zarządzania, w oparciu o przynajmniej: a) ilość znaków, b) czy hasło ma zawierać wielkie litery, c) czy hasło ma zawierać małe litery, d) czy hasło ma zawierać cyfry, e) czy hasło ma zawierać znaki specjalne, f) okres ważności, g) ilość nieudanych logowań." Administrator musi mieć możliwość konfiguracji złożoności haseł dla użytkowników na stacjach roboczych. "Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej: a) ilość znaków, b) czy hasło ma zawierać wielkie litery, c) czy hasło ma zawierać małe litery, d) czy hasło ma zawierać cyfry, e) czy hasło ma zawierać znaki specjalne, f) okres ważności, g) ilość nieudanych logowań, h) możliwość zmiany hasła." "Konsola centralnego zarządzania musi gromadzić informacje o: a) nazwach stacji roboczych, na których jest zainstalowany klient systemu szyfrowania danych, b) dacie ostatniej modyfikacji ustawień klienta systemu szyfrowania danych, c) dacie aktywacji klienta systemu szyfrowania danych, d) statusu szyfrowania, e) typie urządzenia na którym jest zainstalowany klient systemu szyfrowania danych, f) stanie polityki, g) wersji klienta systemu szyfrowania danych, h) wersji systemu operacyjnego stacji roboczej, i) użytkownikach uprawnionych do logowania do oprogramowania na stacji roboczej." Konsola centralnego zarządzania musi pozwalać na wygenerowanie dla każdej zaszyfrowanej stacji płyty ratunkowej. Konsola musi być dostępna z poziomu interfejsu WWW. Administrator musi mieć możliwość zarządzania stacjami klienckimi, które mają dostęp do sieci Internet. Administrator musi mieć możliwość konfiguracji automatycznego szyfrowania pełnej powierzchni dysku po wykonanej instalacji oprogramowania.

Załącznik - Nr 1

	Konsola centralnego zarządzania musi posiadać możliwość automatycznej aktywacji licencji w ramach kont domenowych. "Administrator musi mieć możliwość wykonania poniższych czynności w sposób zdalny: a) instalacji klienta na stacji, b) zaszyfrowania/odszyfrowania stacji, c) wygenerowania klucza aktywacyjnego dla użytkownika, d) administrowania kluczami szyfrującymi, e) administrowania użytkownikami, którzy mają dostęp do stacji, f) administrowania profilem ustawień dla użytkowników, g) administrowania profilem ustawień dla stacji roboczych, h) wymuszenia zmiany hasła, i) zarządzania wieloma organizacjami z poziomu jednej konsoli." WYMAGANIA SYSTEMOWE APLIKACJI KLIENCKIEJ System szyfrowania danych musi wspierać instalacje aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10/11 oraz w środowiskach Microsoft Windows Server 2012, 2012 R2, 2016, 2019, 2022. System musi posiadać certyfikat FIPS 140-2 Level 1 WYMAGANIA DOTYCZĄCE UWIERZYTELNIANIA Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Aplikacja musi umożliwiać określenie, co najmniej 127 unikalnych użytkowników, którzy będą mieć dostęp do chronionej stacji roboczej na poziomie Pre-Boot. Aplikacja musi umożliwiać przetrzymywanie, co najmniej 64 kluczy szyfrujących w jednym pęku kluczy (key file). Dostęp do pliku klucza musi być chroniony przy pomocy hasła. Domyślnie wykorzystywane hasło musi być hasłem systemu Windows. Administrator musi posiadać możliwość modyfikacji ekranu logowania (Pre-boot). WYMAGANIA DOTYCZĄCE USTAWIEŃ APLIKACJI KLIENCKIEJ Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim. Defragmentacja dysku nie może mieć negatywnego wpływu na system szyfrowania. "Aplikacja musi umożliwiać szyfrowanie nośników wymiennych w następujący sposób: a) sektor po sektorze, b) kontener." Zaszyfrowany nośnik wymienny oraz nośnik CD/DVD może być odczytany na dowolnej stacji, na której nie ma zainstalowanego klienta systemu szyfrowania. Dostęp do takiego nośnika musi być możliwy po podaniu hasła. Aplikacja musi pozwalać na szyfrowanie wiadomości e-mail wraz z załącznikami. Aplikacja musi umożliwiać automatyczną deszyfrację otrzymywanych wiadomości e-mail. Aplikacja musi pozwalać na szyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego. Zaszyfrowany tekst może być odczytany, za pomocą narzędzia, dostarczanego przez producenta, na stacji bez zainstalowanego klienta systemu szyfrowania. Aplikacja musi umożliwiać wybór klucza szyfrującego (w przypadku posiadania wielu kluczy w pęku), który ma być używany w procesie szyfrowania. Aplikacja musi umożliwiać wybór domyślnego klucza szyfrowania. Aplikacja musi umożliwiać zaszyfrowanie pliku lub folderu z poziomu menu kontekstowego. Możliwe jest utworzenie skrótów klawiszowych umożliwiających zaszyfrowanie/odszyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego. Aplikacja musi umożliwiać tworzenie wirtualnych partycji. Dostęp do takich partycji ma być możliwy przy użyciu klucza szyfrującego lub hasła. Aplikacja musi umożliwiać zdefiniowanie wielkości wirtualnej partycji, z dokładnością do 1MB. Aplikacja musi umożliwiać tworzenie zaszyfrowanego archiwum. Dostęp do takiego archiwum ma być możliwy, przy użyciu klucza szyfrującego lub hasła. "Aplikacja musi umożliwiać trwałe usuwanie danych za pomocą poniższych algorytmów: a) Guttman. b) US Department of Defence 5220.22-M (8-306. /E). c) US Department of Defence 5220.22-M (8-306. /E, CiE). d) Kryptograficzne losowe dane liczbowe." Aplikacja musi posiadać dedykowaną wtyczkę co najmniej dla klientów pocztowych MS Outlook 2003 lub nowszych, również dostępnych z poziomu Office 365. Aplikacja musi umożliwiać automatyczne zalogowanie użytkownika do pęku klucza (key file) systemu szyfrowania danych po uruchomieniu systemu operacyjnego. Aplikacja musi umożliwiać automatyczne wylogowanie z aplikacji w przypadku bezczynności użytkownika w systemie. Aplikacja musi posiadać opcję automatycznego odpytywania serwerów producenta o dostępność nowszych wersji. Użytkownik musi posiadać możliwość ręcznego sprawdzania czy dostępna jest nowsza wersja programu, z poziomu GUI. WYMAGANIA DOTYCZĄCE SZYFROWANIA Aplikacja musi dawać możliwość szyfrowania powierzchni dysku sektor po sektorze. Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM. Aplikacja musi umożliwiać wstrzymanie procesu szyfrowania powierzchni dysku i jego wznowienie. Proces szyfrowania danych powinien rozpocząć się od momentu, w którym został przerwany.

Załącznik - Nr 1

	Aplikacja musi umożliwiać wstrzymanie procesu szyfrowania, w sytuacji gdy laptop nie jest podłączony do zasilania. Proces szyfrowania musi zostać wznowiony automatycznie, po podłączeniu zasilacza. "Wymagane jest wykorzystanie kluczy szyfrujących, utworzonych przy użyciu jednego z poniższych algorytmów szyfrowania: a) AES (Rijndael). b) Blowfish. c) Triple DES (3DES)." Aplikacja musi umożliwiać współpracę z dyskami SSD. Aplikacja musi umożliwiać współpracę z dyskami sprzętowo szyfrowanymi, działającymi w technologii TCG OPAL. Aplikacja musi umożliwiać szyfrowanie danych na komputerach z UEFI. Administrator musi mieć możliwość sprawdzenia, przed zaszyfrowaniem całej powierzchni dysku, czy nie pojawią się problemy po ponownym uruchomieniu komputera. Administrator musi mieć możliwość opcjonalnego szyfrowania niesystemowych partycji dysku. WYMAGANIA DOTYCZĄCE SYTUACJI KRYTYCZNYCH W przypadku utraty hasła, aplikacja musi umożliwiać Administratorowi odzyskanie dostępu do zaszyfrowanego dysku poprzez użycie zdefiniowanego wcześniej hasła administratora. W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania. **Urząd Gminy Luzino posiada licencje ESET PROTECT Entry ON-PREM w ilości 85 stanowisk. Zamawiając dopuszcza upgrade posiadanych przez zamawiającego licencji.** **Okres trwania licencji: 24 miesiące.**