Załącznik Nr 1

do zapytania ofertowego

**OPIS PRZEDMIOTU ZAMÓWIENIA**

|  |  |  |
| --- | --- | --- |
| **Przenośna stacja robocza** | | |
| **W ofercie należy wpisać Producent, model, nr produktu producenta komputera: [tutaj wpisać]** | | |
| **Parametr** | **Minimalne wymagane parametry** | **Szczegółowy opis oferowanego przedmiotu, umożliwiający identyfikację** |
| Ekran | matowy jasność 250 nitów, 15” |  |
| Procesor | Osiągający wydajność 13195 pkt wg CPU Mark PassMark Software przy 25 próbkach. Do oferty dołączyć potwierdzający wydruk testu lub dokumentację producenta. |  |
| Obudowa | Z boku obudowy wyprowadzone fabrycznie: złącze zasilania; video 3840×2160 przy 24, 25, 30 Hz, 1920×1080 przy 120 Hz; 3 x USB w tym 2 x USB 3.2; złącze słuchawek i mikrofonu; czytnik kart MMC SD; diodowy wskaźnik zasilania; |  |
| Wyposażenie fabryczne | Pamięć 8GB DDR4; dysk 480GB SSD; mikrofon tablicowy; kamera z przesłoną i ustawianym skupieniem; dwa głośniki z systemem Dolby; bluetooth 5.0; zasilacz sieciowy PL 230V; |  |
| Karta graficzna | Możliwość korzystania z dwóch niezależnych wyświetlaczy |  |
| Fabryczna Gwarancja producenta | 24 miesiące i zapewniona możliwość aktualizacji oprogramowania komputera do 2027 r.  Warunki gwarancji producenta dla wymiany sprzętu na nowy w przypadku uszkodzenia ekranu:  Jasne subpixele =<2 w tym zielony =0; ciemne subpixele =<3; odległość wadliwych niepodświetlonych pixeli nie może przekraczać 5mm |  |
| Inne | Obsługa pamięci DDR4-3200; obsługa dwóch wewnętrznych dysków SSD; wydajność baterii: praca 7 godzin, a przy oglądaniu video 8,5 godziny wg testu MobileMark, naładowanie baterii do 80% w ciągu 1 godziny - do oferty dołączyć potwierdzający wydruk testu lub dokumentację producenta; zintegrowana klawiatura numeryczna i touchpad bez przycisków; waga poniżej 2,2kg grubość poniżej 2cm; przedmiot zamówienia musi być fabrycznie nowy; |  |
| Oprogramowanie | System operacyjny o funkcjonalnościach:  Możliwość dokonywania aktualizacji i poprawek systemu przez Internet; możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat); Internetowa aktualizacja zapewniona w języku polskim; Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPSec v4 i v6; Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, klient poczty elektronicznej, sklep z aplikacjami; Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (np.: drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); System działa w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta; Zabezpieczony hasłem hierarchiczny dostęp do systemu, praca systemu w trybie ochrony kont użytkowników; Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych; Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie; Obsługa szyfrowania dysków uniemożliwiająca nieautoryzowany dostęp do urządzenia lub danych; System operacyjny posiada wbudowaną funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika; Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi; Wbudowany system pomocy w języku polskim; System operacyjny fabrycznie zainstalowany przez producenta komputera z pomocą techniczną producenta komputera świadczoną w języku polskim przez chat internetowy i przez telefon, w ofercie podać nr telefonu i link do pomocy; System operacyjny fabrycznie zainstalowany przez producenta komputera z pomocą techniczną producenta systemu operacyjnego świadczoną w języku polskim przez internet i przez telefon, w ofercie podać nr telefonu i link do pomocy; System operacyjny musi zapewniać synchronizację komputera ze smartfonem Apple i Android; System operacyjny musi zapewniać wbudowany „sklep” internetowy w języku polskim z różnymi dodatkami instalacyjnymi (aplikacjami) zwiększającymi możliwości standardowego systemu operacyjnego; System operacyjny powinien być wyposażony w możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509, certyfikat EAL 4 dla systemu operacyjnego zarządzanych w sposób centralny; Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń; Graficzne środowisko instalacji i konfiguracji; Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; Możliwość przywracania plików systemowych z kopii zapasowej.  Program antywirusowy z licencją do 2027 r. o funkcjonalności: monitorowanie procesów plików, zmiany plików i rejestru oraz inne zdarzenia w punktach końcowych pod kątem podejrzanej i znanej złośliwej aktywności, silnik antywirusowy odnotowuje wszelkie zmiany w plikach (zapisy plików, takie jak przenoszenie, kopie lub modyfikacje) oraz ogólną aktywność programu (otwarte lub uruchomione programy, które powodują uruchamianie innych programów), informacje o nieprzetworzonych zapisach objętości, określanie maksymalnego rozmiaru pobieranych plików i załączników do skanowania, ochrona w chmurze, ochrona sieci chroni przed zdarzeniami internetowymi - zdolność redukcji ataku - zapobiega dostępowi do niebezpiecznych domen, które zawierają oszustwa phishingowe, exploity i inną złośliwą zawartość w Internecie, ochrona przed: uruchamianiem plików wykonywalnych i skryptów, które próbują pobrać lub uruchomić pliki, uruchamianie zaciemnionych lub w inny sposób podejrzanych skryptów, wykonywaniem zachowań, których aplikacje zwykle nie inicjują podczas normalnej codziennej pracy, konfigurowane opcje naprawcze po wykryciu zagrożenia: punkt przywracania, usuwanie elementu, kwarantanna określana przez ilość dni. Powyższy program antywirusowy fabrycznie zainstalowany przez producenta komputera z pomocą techniczną producenta oprogramowania świadczoną w języku polskim przez internet i przez telefon, w ofercie podać nr telefonu i link do pomocy.  Odrębny od systemu operacyjnego program do tworzenia kopii zapasowych z wieczystą licencją o funkcjonalności: kopia zapsowa składowana na dysku lokalnym, sieciowym, w chmurze OneDrive, w chmurze producenta programu; możliwość tworzenia wielu niezależnych zadań backupowych; zapewniona przez producenta aktualizacja oprogramowania w czasie tzw. life time; zajętość dysku przy instalacji poniżej 200MB; kompatybilność z BIOS i UEFI i BitLocker i Windows 10 wydanie 1809, 1803, 1507, 1607; zapis kopi zapasowych na dysk komputera, DAS, USB, eSATA, FireWire, RDM, NAS poprzez CIFS, SAN, iSCSI; działanie programu sygnalizowane przez ikonę w pasku „tray” z szybkim dostępęm wywoływanym myszą do funkcji: backup (backup teraz, pełny backup, osobny pełny backup, backup do innej lokalizacji, konfiguracja backupu), przywracanie (pojedyncze pliki, cały dysk lub prarycję), panel sterowania programem; tworzenie rozruchowego dysku odzyskiwania systemu Windows z zapisem do pliku iso i na USB; przenoszenie i odtwarzanie (bez instalacji) całego gotowego systemu operacyjnego ze starego komputera na nowy, nawet na zupełnie inny dysk i komputer; wbudowany menedżer dysku do zwiększania i zmniejszania rozmiaru partycji; kopie zapasowe danych wykonywane na żądanie oraz według harmonogramu czasowego oraz wyzwalane po podłączeniu lokalizacji docelowej; podczas działania programu na ekranie widoczne informacje: planowy i aktualny czas trwania backupu, rozmiar backupu, rozmiar miejsca docelowego i pozostałe wolne miejsce, prędkość odczytu danych, programowe przyspieszanie backupu podczas zajętości systemu operacyjnego; włączane i wyłączane powiadomienia mailowe z programu backupu; możliwość nadania nazwy i opisu dla każdego zadania backupu; wybierany format kopii zapasowej: cały komputer łącznie z podłączonymi dyskami USB, poszczególne partycje, tylko system operacyjny i ukryte partycje sprzętowe, poszczególne pliki i katalogi z możliwością tzw. maskowania nazw plików do kilku lub pojedynczych liter; dowolnie ustawiany czas retencji kopii zapasowej; ustawiane cykliczne wywoływanie aktywnego pełnego backupu co do dnia (miesięczne, tygodniowe, dzienne); ustawiane sprawdzanie poprawności kopii zapasowej co do dnia (miesięczne, tygodniowe, dzienne, auto); wybierane 4 metody kompresji; deduplikacja kopii zasowej; ustawiany harmonogram kopii zapasowych (cykliczny co do dnia i godziny, tylko w określone dni, zależny od stanu komputera włączenie/wyłączenie tzn. kopia tworzona zaraz po włączeniu komputera oraz komputer wyłączany po zrobieniu kopii, wyzwalanie kopii po zamknięciu, wylogowaniu, podłączeniu dysku USB lub NAS); szyfrowanie kopii zapasowej; wywoływanie kopii zapasowej zaraz po skonfigurowaniu danego zadania backupu; automatyczne szukanie plików możliwych do odzyskania po uruchomieniu funkcji przywracania danych; wybieranie dowolnego punktu przywracania danych. |  |

|  |  |  |
| --- | --- | --- |
| **Stacja robocza** | | |
| **W ofercie należy wpisać Producent, model, nr produktu producenta komputera: [tutaj wpisać]** | | |
| **Parametr** | **Minimalne wymagane parametry** | **Szczegółowy opis oferowanego przedmiotu, umożliwiający identyfikację** |
| Ekran | Bezramkowy FHD matowy jasność 250 nitów; ponad 23”; kąty widzenia 90 st. +/- 1 st. |  |
| Procesor | Osiągający wydajność 13195 pkt wg CPU Mark PassMark Software przy 25 próbkach. Do oferty dołączyć potwierdzający wydruk testu lub dokumentację producenta. |  |
| Obudowa | Z tyłu obudowy wyprowadzone fabrycznie: złącze i przycisk zasilania; video 3840×2160 przy 24, 25, 30 Hz, 1920×1080 przy 120 Hz; 4 x USB w tym 2 x USB 3.2 Gen 1; RJ45. Czytnik kart MMC SD. Napęd optyczny DVDRW. |  |
| Wyposażenie fabryczne | Pamięć 2 x 8GB DDR4; dysk 500GB SSD PCIe 3.0; kamera 720p z ustawianym skupieniem; głośniki z systemem HD 6W; bluetooth 5.0; energooszczędny zasilacz sieciowy 230V o wydajności ponad 85%; wbudowany mikrofon; bezprzewodowa klawiatura i mysz; |  |
| Karta graficzna | Możliwość korzystania z dwóch niezależnych wyświetlaczy |  |
| Fabryczna Gwarancja producenta | 24 miesiące i zapewniona możliwość aktualizacji oprogramowania komputera do 2027 r.  Warunki gwarancji producenta dla wymiany sprzętu na nowy w przypadku uszkodzenia ekranu: uszkodzone piksele =0 lub jasne subpiksele >2 lub ciemne subpiksele >5 lub liczba subpikseli >5. |  |
| Inne | Certyfikaty: EnergyStar 8.0, ErP 7; Obsługa pamięci DDR4-3200; obsługa dwóch wewnętrznych dysków SSD; waga poniżej 7 kg; wymiary poniżej 55x19x45 cm; przedmiot zamówienia musi być fabrycznie nowy; |  |
| Oprogramowanie | System operacyjny o funkcjonalnościach:  Możliwość dokonywania aktualizacji i poprawek systemu przez Internet; możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat); Internetowa aktualizacja zapewniona w języku polskim; Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPSec v4 i v6; Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, klient poczty elektronicznej, sklep z aplikacjami; Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (np.: drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); System działa w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta; Zabezpieczony hasłem hierarchiczny dostęp do systemu, praca systemu w trybie ochrony kont użytkowników; Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych; Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie; Obsługa szyfrowania dysków uniemożliwiająca nieautoryzowany dostęp do urządzenia lub danych; System operacyjny posiada wbudowaną funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika; Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi; Wbudowany system pomocy w języku polskim; System operacyjny fabrycznie zainstalowany przez producenta komputera z pomocą techniczną producenta komputera świadczoną w języku polskim przez chat internetowy i przez telefon, w ofercie podać nr telefonu i link do pomocy; System operacyjny fabrycznie zainstalowany przez producenta komputera z pomocą techniczną producenta systemu operacyjnego świadczoną w języku polskim przez internet i przez telefon, w ofercie podać nr telefonu i link do pomocy; System operacyjny musi zapewniać synchronizację komputera ze smartfonem Apple i Android; System operacyjny musi zapewniać wbudowany „sklep” internetowy w języku polskim z różnymi dodatkami instalacyjnymi (aplikacjami) zwiększającymi możliwości standardowego systemu operacyjnego; System operacyjny powinien być wyposażony w możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509, certyfikat EAL 4 dla systemu operacyjnego zarządzanych w sposób centralny; Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń; Graficzne środowisko instalacji i konfiguracji; Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; Możliwość przywracania plików systemowych z kopii zapasowej.  Program antywirusowy z licencją do 2027 r. o funkcjonalności: monitorowanie procesów plików, zmiany plików i rejestru oraz inne zdarzenia w punktach końcowych pod kątem podejrzanej i znanej złośliwej aktywności, silnik antywirusowy odnotowuje wszelkie zmiany w plikach (zapisy plików, takie jak przenoszenie, kopie lub modyfikacje) oraz ogólną aktywność programu (otwarte lub uruchomione programy, które powodują uruchamianie innych programów), informacje o nieprzetworzonych zapisach objętości, określanie maksymalnego rozmiaru pobieranych plików i załączników do skanowania, ochrona w chmurze, ochrona sieci chroni przed zdarzeniami internetowymi - zdolność redukcji ataku - zapobiega dostępowi do niebezpiecznych domen, które zawierają oszustwa phishingowe, exploity i inną złośliwą zawartość w Internecie, ochrona przed: uruchamianiem plików wykonywalnych i skryptów, które próbują pobrać lub uruchomić pliki, uruchamianie zaciemnionych lub w inny sposób podejrzanych skryptów, wykonywaniem zachowań, których aplikacje zwykle nie inicjują podczas normalnej codziennej pracy, konfigurowane opcje naprawcze po wykryciu zagrożenia: punkt przywracania, usuwanie elementu, kwarantanna określana przez ilość dni. Powyższy program antywirusowy fabrycznie zainstalowany przez producenta komputera z pomocą techniczną producenta oprogramowania świadczoną w języku polskim przez internet i przez telefon, w ofercie podać nr telefonu i link do pomocy.  Odrębny od systemu operacyjnego program do tworzenia kopii zapasowych z wieczystą licencją o funkcjonalności: kopia zapsowa składowana na dysku lokalnym, sieciowym, w chmurze OneDrive, w chmurze producenta programu; możliwość tworzenia wielu niezależnych zadań backupowych; zapewniona przez producenta aktualizacja oprogramowania w czasie tzw. life time; zajętość dysku przy instalacji poniżej 200MB; kompatybilność z BIOS i UEFI i BitLocker i Windows 10 wydanie 1809, 1803, 1507, 1607; zapis kopi zapasowych na dysk komputera, DAS, USB, eSATA, FireWire, RDM, NAS poprzez CIFS, SAN, iSCSI; działanie programu sygnalizowane przez ikonę w pasku „tray” z szybkim dostępęm wywoływanym myszą do funkcji: backup (backup teraz, pełny backup, osobny pełny backup, backup do innej lokalizacji, konfiguracja backupu), przywracanie (pojedyncze pliki, cały dysk lub prarycję), panel sterowania programem; tworzenie rozruchowego dysku odzyskiwania systemu Windows z zapisem do pliku iso i na USB; przenoszenie i odtwarzanie (bez instalacji) całego gotowego systemu operacyjnego ze starego komputera na nowy, nawet na zupełnie inny dysk i komputer; wbudowany menedżer dysku do zwiększania i zmniejszania rozmiaru partycji; kopie zapasowe danych wykonywane na żądanie oraz według harmonogramu czasowego oraz wyzwalane po podłączeniu lokalizacji docelowej; podczas działania programu na ekranie widoczne informacje: planowy i aktualny czas trwania backupu, rozmiar backupu, rozmiar miejsca docelowego i pozostałe wolne miejsce, prędkość odczytu danych, programowe przyspieszanie backupu podczas zajętości systemu operacyjnego; włączane i wyłączane powiadomienia mailowe z programu backupu; możliwość nadania nazwy i opisu dla każdego zadania backupu; wybierany format kopii zapasowej: cały komputer łącznie z podłączonymi dyskami USB, poszczególne partycje, tylko system operacyjny i ukryte partycje sprzętowe, poszczególne pliki i katalogi z możliwością tzw. maskowania nazw plików do kilku lub pojedynczych liter; dowolnie ustawiany czas retencji kopii zapasowej; ustawiane cykliczne wywoływanie aktywnego pełnego backupu co do dnia (miesięczne, tygodniowe, dzienne); ustawiane sprawdzanie poprawności kopii zapasowej co do dnia (miesięczne, tygodniowe, dzienne, auto); wybierane 4 metody kompresji; deduplikacja kopii zasowej; ustawiany harmonogram kopii zapasowych (cykliczny co do dnia i godziny, tylko w określone dni, zależny od stanu komputera włączenie/wyłączenie tzn. kopia tworzona zaraz po włączeniu komputera oraz komputer wyłączany po zrobieniu kopii, wyzwalanie kopii po zamknięciu, wylogowaniu, podłączeniu dysku USB lub NAS); szyfrowanie kopii zapasowej; wywoływanie kopii zapasowej zaraz po skonfigurowaniu danego zadania backupu; automatyczne szukanie plików możliwych do odzyskania po uruchomieniu funkcji przywracania danych; wybieranie dowolnego punktu przywracania danych. |  |

|  |  |
| --- | --- |
| **Pakiet biurowy** | |
| **W ofercie należy wpisać Producent, model, nr produktu producenta: [tutaj wpisać]** | |
| **Minimalne wymagane parametry** | **Szczegółowy opis oferowanego przedmiotu, umożliwiający identyfikację** |
| Pełna wersja pakietu oprogramowania użytkowego o funkcjonalnościach:  1 Interfejs użytkownika:  a. pełna polska wersja językowa interfejsu użytkownika;  b. prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych;  2 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 (Dz. U. 2012, poz. 526);  3 Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców;  4 W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy);  5 Do aplikacji musi być dostępna pełna dokumentacja w języku polskim;  6 Pakiet zintegrowanych aplikacji biurowych musi zawierać:  a. edytor tekstów;  b. arkusz kalkulacyjny;  c. narzędzie do przygotowywania i prowadzenia prezentacji;  d. narzędzie do tworzenia drukowanych materiałów informacyjnych;  e. narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami);  f. narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.  7 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; zapisywanie i otwieranie plików pdf;  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);  k. wydruk dokumentów;  l. wykonywanie korespondencji seryjnej, bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną;  m. prace na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu;  n. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzeniem modyfikacji;  o. wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa;  8 Arkusz kalkulacyjny musi umożliwiać:  a. tworzenie raportów tabelarycznych;  b. tworzenie wykresów liniowych (wraz z 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, webservice);  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 zmianę 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 2003 oraz Microsoft Excel 2007 i 2010, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń;  n. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzeniem modyfikacji.  9 Narzędzie do przygotowywania i prowadzenia prezentacji multimedialnych musi umożliwiać:  a. przygotowywanie prezentacji multimedialnych;  b. prezentowanie przy użyciu projektora multimedialnego;  c. drukowanie w formacie umożliwiającym robienie notatek;  d. zapisanie jako prezentacji 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 2003, MS PowerPoint 2007 i 2010.  10 Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:  a. tworzenie i edycję drukowanych materiałów informacyjnych;  b. tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów;  c. edycję poszczególnych stron materiałów;  d. podział treści na kolumny;  e. umieszczanie elementów graficznych;  f. wykorzystanie mechanizmu korespondencji seryjnej;  g. płynne przesuwanie elementów po całej stronie publikacji;  h. eksport publikacji do formatu PDF oraz TIFF;  i. wydruk publikacji;  j. możliwość przygotowywania materiałów do wydruku w standardzie CMYK.  11. Pomoc techniczna producenta oprogramowania świadczoną w języku polskim przez internet i przez telefon, w ofercie podać nr telefonu i link do pomocy.  12 Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:  a. pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego;  b. filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określenie listy zablokowanych i bezpiecznych nadawców;  c. tworzenie katalogów, pozwalających katalogować pocztę elektroniczną;  d. automatyczne grupowanie poczty o tym samym tytule;  e. tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy;  f. oflagowanie poczty elektronicznej z określeniem terminu przypomnienia;  g. zarządzanie kalendarzem;  h. udostępnianie kalendarza innym użytkownikom;  i. przeglądanie kalendarza innych użytkowników;  j. zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach;  k. zarządzanie listą zadań;  l. zlecanie zadań innym użytkownikom;  m. zarządzanie listą kontaktów;  n. udostępnianie listy kontaktów innym użytkownikom;  o. przeglądanie listy kontaktów innych użytkowników;  p. możliwość przesyłania kontaktów innym użytkownikom. |  |

|  |  |
| --- | --- |
| **System ochrony sieci** | |
| **W ofercie należy wpisać Producent, model, nr produktu producenta: [tutaj wpisać]** | |
| **Minimalne wymagane parametry** | **Szczegółowy opis oferowanego przedmiotu, umożliwiający identyfikację** |
| Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. System realizujący funkcję ochrony sieci musi dawać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System musi wspierać IPv4 oraz IPv6 w zakresie: Ochrony w warstwie aplikacji, Protokołów routingu dynamicznego. W przypadku systemu pełniącego funkcje: IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster active-active lub active-passive. W obu trybach powinna istnieć funkcja synchronizacji sesji ochrony siecil. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System realizujący funkcję ochrony sieci musi dysponować minimum 10 portami Gigabit Ethernet RJ-45. System ochrony sieci musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. W ramach systemu ochrony sieci powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. W zakresie frewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. Przepustowość stateful dla ochrony sieci: nie mniej niż 10 Gbps dla pakietów 512 B. Przepustowość ochrony sieci z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: Kontrola dostępu - zapora ogniowa klasy Stateful Inspection; Kontrola Aplikacji; Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN; Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS; Ochrona przed atakami - Intrusion Prevention System; Kontrola stron WWW; Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3; Zarządzanie pasmem (QoS, Traffic shaping); Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP); Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site; Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2; Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. Polityka ochrony sieci musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: Translację jeden do jeden oraz jeden do wielu; Dedykowany ALG (Application Level Gateway) dla protokołu SIP. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP, nazwy domenowe, hashe złośliwych plików. Element systemu realizujący funkcję ochrony sieci musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu: Amazon Web Services (AWS); Microsoft Azure ; Google Cloud Platform (GCP); OpenStack; VMware NSX; System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: Wsparcie dla IKE v1 oraz v2; Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM); Obsługa protokołu Diffie-Hellman grup 19 i 20; Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE; Tworzenie połączeń typu Site-to-Site oraz Client-to-Site; Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności; Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego; Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth; Mechanizm „Split tunneling” dla połączeń Client-to-Site. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0; Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta; Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. W zakresie routingu rozwiązanie powinno zapewniać obsługę: Routingu statycznego; Policy Based Routingu; Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. System ochrony sieci musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. Moduł kontroli WWW musi korzystać z bazy adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. System ochrony sieci musi umożliwiać weryfikację tożsamości użytkowników za pomocą: Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu; Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP; Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. Element systemu pełniący funkcję ochrony sieci musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji ochrony sieci. Element systemu realizujący funkcję ochrony sieci musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. W ramach logowania system pełniący funkcję ochrony siecil musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Musi istnieć możliwość logowania do serwera SYSLOG. Z urządzeniem należy dostarczyć licencje upoważniające do korzystania w okresie gwarancji na urządzenie z aktualnych baz funkcji ochronnych producenta i serwisów w zakresie: kontrola aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzęń mobilnych - co najmniej dla systemu operacyjnego Android), analiza typu Sandbox, antyspam, web filtering, bazy reputacyjne adresów IP/domen. Trzyletnia gwarancja producenta. Dostawa nowego urządzenia do 8 godzin od awarii. Wsparcie w reżimie 24x7 w językach angielskim i polskim. W ramach dostawy wykonawca dokona pełnego wdrożenia oferowanego przedmiotu zamówienia wg wytycznych Zamawiającego. |  |

|  |  |
| --- | --- |
| **Szkolenie stacjonarne dla pracowników urzędu w zakresie obsługi zakupionego sprzętu i oprogramowania** | |
|  | |
| **Minimalne wymagane parametry** | **Szczegółowy opis oferowanego przedmiotu, umożliwiający identyfikację** |
| * Poruszania się w środowisku Windows * Używania funkcji i programów wbudowanych w system * Poprawnej instalacji systemu operacyjnego * Zaawansowanej obsługi systemu operacyjnego * Aktualizacji i bezpieczeństwa w środowisku Windows * Korzystania z apletu Narzędzia administracyjne |  |

|  |  |
| --- | --- |
| **Diagnoza cyberbezpieczeństwa** | |
|  | |
| **Minimalne wymagane parametry** | **Szczegółowy opis oferowanego przedmiotu, umożliwiający identyfikację** |
| 1. Wykonawca przeprowadzi diagnozę cyberbezpieczeństwa jednostki samorządu terytorialnego – Urzędu Gminy Ludwin.  2. Diagnoza musi być przeprowadzona w zakresie określonym w „Formularzu informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa” stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego Cyfrowa Gmina  3. Diagnoza musi być przeprowadzona przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.  4. Wykonawca przekaże wynik przeprowadzonej diagnozy w postaci pliku wypełnionego arkusza kalkulacyjnego formularza, o którym mowa w pkt. 2, podpisanego podpisem cyfrowym (weryfikowanym certyfikatem kwalifikowanym lub przy wykorzystaniu profilu zaufanego) przez osobę posiadającą uprawnienia, o których mowa w pkt. 3.  5. Jednostki samorządu terytorialnego biorące udział w projekcie „Cyfrowa Gmina” są zobowiązane do przeprowadzenia diagnozy cyberbezpieczeństwa będącej przedmiotem niniejszego zamówienia. Niezwłocznie po jej przeprowadzeniu, jej wyniki mają być przekazane przez Zamawiającego do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK) za pośrednictwem platformy ePUAP. Dane z diagnozy przekazane przez JST do NASK posłużą do opracowania raportu na temat stanu bezpieczeństwa systemów jednostek samorządowych. Wykonawca jest zobowiązany mieć na uwadze powyższy cel przeprowadzenia diagnozy i jej przeznaczenie. |  |