OPIS PRZEDMIOTU ZAMÓWIENIA

I. PRZEDMIOT ZAMÓWIENIA:

Przedmiotem zamówienia jest **Dostawa sprzętu komputerowego, oprogramowania oraz urządzeń peryferyjnych do Podlaskiej Wojewódzkiej Komendy OHP i jej jednostek organizacyjnych**

Zamówienie składa się **z III części zamówienia**:

- **Część I** – Dostawa sprzętu komputerowego z oprogramowaniem oraz urządzeń peryferyjnych.
- **Część II** – Dostawa licencji na oprogramowanie antywirusowe ESET Protect Entry lub równoważne
- **Część III** – Dostawa licencji bezpieczeństwa Unified Threat Protection (UTP) dla urządzenia FortiGate-100F.

II. SZCZEGÓŁY DOT. WYKONANIA DOSTAWY ZAMÓWIENIA:

Termin realizacji:

Cześć 1 – **10 dni roboczych od dnia akceptacji zestawienia**

Część 2 **- do 14 dni roboczych od dnia popisania umowy**

Część 3 - **do 10 dni roboczych od dnia popisania umowy**

Wykonawca przeprowadzi dostawę przedmiotu zamówienia w dniach roboczych w godzinach 8.00-14.00.

Wypłata wynagrodzenia za wykonanie przedmiotu zamówienia, nastąpi przelewem na rachunek bankowy Wykonawcy, wskazany na fakturze w terminie 30 dni od jej wystawienia.

Podstawę do wystawienia przez Wykonawcę faktury stanowić będzie podpisany bez zastrzeżeń przez Zamawiającego i Wykonawcę **Protokół odbioru dostawy** stanowiący załącznik do umowy. Dla każdej z części zamówienia podpisany zostanie odrębny Protokół odbioru dostawy.

Za datę zapłaty uznaje się datę obciążenia rachunku bankowego Zamawiającego.

W przypadku części II i części III licencje na oprogramowanie oraz certyfikaty mają zostać dostarczone w formie elektronicznej na podany przez Zamawiającego adres e-mail. W przypadku certyfikatów zawierających klucze licencyjne powinny zostać one zabezpieczone hasłem przez Wykonawcę. Hasła należy przekazać wskazanemu pracownikowi działu IT Zamawiającego.

Części zamówienia i adresy dostawy:

Część zamówienia	Przedmiot zamówienia	Adres dostawy
Część I	Dostawa sprzętu komputerowego z oprogramowaniem oraz urządzeń peryferyjnych	Podlaska Wojewódzka Komenda OHP w Białymstoku, ul. Trawiasta 20B, 15-161 Białystok
Część II	Dostawa licencji na oprogramowanie antywirusowe ESET Protect Entry lub równoważne	Podlaska Wojewódzka Komenda OHP w Białymstoku, ul. Trawiasta 20B, 15-161 Białystok e-mail: it@podlaska.ohp.pl
Część III	Dostawa licencji bezpieczeństwa Unified Threat Protection (UTP) dla urządzenia FortiGate-100F	Podlaska Wojewódzka Komenda OHP w Białymstoku, ul. Trawiasta 20B, 15-161 Białystok e-mail: it@podlaska.ohp.pl

III. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Część I – Dostawa sprzętu komputerowego z oprogramowaniem oraz urządzeń peryferyjnych

W ramach części I Wykonawca ma dostarczyć Zamawiającemu następujący sprzęt komputerowy z oprogramowaniem:

Lp.	Wyszczególnienie	Ilość
1.	Zestaw komputerowy z oprogramowaniem, w skład którego wchodzi: komputer przenośny (laptop) z oprogramowaniem, myszka optyczna przewodowa, klawiatura zewnętrzna przewodowa, replikator portów oraz torba na laptopa Minimalne parametry techniczno-jakościowe określono poniżej.	8 zestawów /minimalny zakres zamówienia 4 zestawy
2.	Monitor komputerowy Minimalne parametry techniczno-jakościowe określono poniżej.	2 sztuki/ minimalny zakres zamówienia 1 sztuka
3.	Urządzenie wielofunkcyjne laserowe monochromatyczne Minimalne parametry techniczno-jakościowe określono poniżej.	2 sztuki
4.	Drukarka laserowa monochromatyczna Minimalne parametry techniczno-jakościowe określono poniżej.	2 sztuki

W przypadku zestawów komputerowych z oprogramowaniem Zamawiający dopuszcza możliwość zmiany ilości zamawianych zestawów komputerowych, minimalny zakres zamówienia to 4 zestawy, w przypadku monitorów komputerowych minimalny zakres zamówienia to 1 sztuka.

MINIMALNE PARAMETRY TECHNICZNO-JAKOŚCIOWE ZESTAWU KOMPUTEROWEGO Z OPROGRAMOWANIEM

Typ	**ZESTAW KOMPUTEROWY Z OPROGRAMOWANIEM** Komputer przenośny (laptop) z oprogramowaniem, myszka optyczna przewodowa, klawiatura zewnętrzna przewodowa, replikator portów oraz torba na komputer przenośny.
Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do Internetu oraz poczty elektronicznej.
Procesor	Procesor o średniej wydajności ocenianej na minimum 12900 pkt (lub więcej) w teście wielowątkowym według Passmark CPU Benchmarks, którego wyniki są dostępne na stronie internetowej: http://www.cpubenchmark.net/cpu_list.php (tab. Single CPU Systems, kolumna CPU Mark). Zamawiający udostępnia wyniki testów Passmark CPU Benchmarks na dzień 30.10.2026r. w ramach załącznika nr 1 do OPZ. Oferowany procesor powinien osiągnąć wynik minimum 12900 pkt (lub więcej) wg załączonego wykazu. Procesor powinien wspierać sprzętowe funkcje zdalnego zarządzania (typu out-of-band) oraz sprzętowe mechanizmy ochrony bezpieczeństwa.
Płyta główna	Chipset dostosowany do zaoferowanego procesora. Zintegrowane karta dźwiękowa i karta sieciowa. Zintegrowany moduł TPM.
Karta graficzna	Zintegrowana z procesorem z dynamicznie przydzielaną pamięcią współdzieloną.
Pamięć operacyjna	Pojemność min. 16GB.
Dysk twardy	Dysk SSD M.2 PCIe NVMe o pojemności min. 512 GB z możliwością szyfrowania.
Multimedia	Wbudowane głośniki stereo. Wbudowany mikrofon. Wbudowana kamera internetowa.
Łączność sieciowa	Karta sieciowa przewodowa 1Gb/s Ethernet. Karta sieciowa bezprzewodowa Wi-Fi 6 (obsługa standardów IEEE.802.11 a/b/g/n/ac/ax). Moduł Bluetooth w wersji 5.0.
Ekran	Matowy o przekątnej 15,6”. Rozdzielczość 1920x1080 (FullHD). Jasność matrycy 250 nitów.
Porty i złącza	1 złącze HDMI. 2 porty USB typu A, w tym minimum 1 port USB 3.0.

	1 port USB typu C obsługujący transmisje danych i zasilanie urządzenia w standardzie Power Delivery lub rozwiązaniu równoważnym. Złącze karty sieciowej RJ-45. Porty audio: wyjście słuchawek i wejście mikrofonowe lub port combo. Złącze zasilania DC. Wskazane powyżej porty i złącza muszą być fizycznie dostępne w komputerze przenośnym i nie mogą być uzyskane za pomocą przejściówek, adapterów itp.
Zabezpieczenia	Wbudowany moduł szyfrujący TPM 2.0 oraz obsługa Secure Boot.
Klawiatura i touchpad	Klawiatura w standardzie QWERTY programisty, wydzielona klawiatura numeryczna. Wielodotykowy, intuicyjny touchpad.
Zasilanie	Bateria o pojemności minimum 40Wh. Dołączony zasilacz (dedykowany do danego modelu laptopa).
System operacyjny	Zainstalowany system operacyjny Microsoft Windows 11 Professional 64bit PL (dopuszcza się standard OEM) **lub równoważny** z licencją bezterminową, w celu zapewnienia współpracy ze środowiskiem sieciowym i aplikacjami funkcjonującymi u Zamawiającego. Zamawiający określił kryteria równoważności, które zostały opisane poniżej. Dołączony nośnik z oprogramowaniem lub partycja recovery umożliwiająca przywrócenie systemu operacyjnego.
BIOS	BIOS zgodny ze specyfikacją UEFI, z pełną obsługą za pomocą klawiatury i myszki. Powinien umożliwiać (bez uruchamiania systemu operacyjnego) odczytanie z niego: wersji BIOS, nr seryjnego komputera, typu zainstalowanego procesora i jego prędkości, rozmiaru pamięci RAM i jej obsadzenie w slotach DIMM. Powinien umożliwiać ustawienie hasła administratora BIOS-u (Supervisor Password) oraz hasła uruchomieniowego (Power-on Password).
Oprogramowanie biurowe	Dołączone oprogramowanie Microsoft Office LTSC 2024 Professional Plus – wersja edukacyjna **lub równoważne**. Okres trwania licencji – licencja dożywotnia. Zamawiający wymaga dostarczenia jednej zbiorczej licencji na określoną liczbę stanowisk. Zamawiający określił kryteria równoważności, które zostały opisane poniżej. Podlaska Wojewódzka Komenda OHP pozytywnie przeszła weryfikację na Microsoft 365 i posiada tenant usługi Microsoft 365. Oprogramowanie Microsoft Office LTSC 2024 Professional Plus (wersja edukacyjna) powinno zostać zarejestrowane przez Wykonawcę (partnera) w tenancie usługi Microsoft 365 Zamawiającego, skąd Zamawiający pobierze klucze licencyjne.
Certyfikaty i standardy	Deklaracja CE producenta o zgodności elektromagnetycznej i bezpieczeństwa zaoferowanych komputerów przenośnych. Certyfikat ISO 9001 producenta sprzętu. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych.
Wsparcie techniczne	Możliwość sprawdzenia (na stronie internetowej producenta lub telefonicznie) konfiguracji sprzętowej komputera oraz warunków gwarancji

	po podaniu numeru seryjnego lub numeru serwisowego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie internetowej producenta komputera, realizowany poprzez podanie na wymienionej stronie numeru seryjnego, numeru serwisowego lub modelu komputera.
Akcesoria	<u>Klasyczna torba na laptopa:</u> • Na laptopa w rozmiarze 15,6”. • Wykonana ze sztywnego materiału. • Minimum 2 komory, w tym główna komora na laptopa oraz druga komora na akcesoria. Komory zapinane na dwustronne metalowe zamki błyskawiczne. • Paski zapinane na rzepy do zabezpieczenia laptopa wewnątrz torby. • Torba musi posiadać rączkę z miękkim wypełnieniem oraz odpinany pasek na ramię. • Kolor wiodący – czarny. <u>Myszka optyczna:</u> • Myszka pełnowymiarowa o długości minimum 110 mm i szerokości minimum 60 mm, • Przewodowa ze złączem USB typu A, długość przewodu min. 1,8 m. • Minimum dwa przyciski funkcyjne oraz rolka przewijania (scroll). • Rozdzielczość 1000 dpi. • Kolor czarny lub szary. <u>Klawiatura zewnętrzna:</u> • Klawiatura membranowa, klasyczna. • Przewodowa ze złączem USB typu A, długość przewodu min. 1,8m. Niski profil klawiszy. • Klawisze muszą być odporne na ścieranie. • Standard QWERTY programisty. • Wydzielona klawiatura numeryczna. • Kolor czarny. <u>Replikator portów:</u> • Kompatybilny z oferowanym modelem laptopa. • Przyłączany do laptopa za pomocą złącza USB typu C (podłączenie typu Plug&Play). • W przypadku, gdy zaoferowany laptop posiada tylko jeden port USB typu C i laptop jest zasilany przez złącze USB typu C, replikator portów powinien umożliwiać przyłączenie do niego zasilacza od laptopa i zasilanie laptopa poprzez replikator. • Umożliwia przyłączenie minimum 1 monitora zewnętrznego przez złącze HDMI oraz sieci LAN. • Wymagane porty: USB 3.0 typu A – 3 szt., USB 3.0 typu C z Power Delivery – 1 szt., HDMI – 1 szt., RJ-45 (Gigabit Ethernet) – 1 szt.
Gwarancja	Minimum 36 miesięcy gwarancji producenta na komputer przenośny, liczone od dnia podpisania protokołu odbioru końcowego. Minimum 24 miesiące gwarancji na akcesoria dodatkowe, liczone od dnia podpisania protokołu odbioru końcowego.

	Serwis urządzeń ma być realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. W przypadku, gdy naprawa „on-site" nie jest możliwa i sprzęt musi zostać przekazany do serwisu zewnętrznego, Wykonawca zapewnia pełną obsługę logistyczną (transport urządzenia w obie strony w systemie Door-to-Door) na własny koszt i ryzyko. W przypadku awarii nośnika danych, Zamawiający zastrzega sobie prawo do zatrzymania uszkodzonego nośnika danych (dysk pozostaje własnością Zamawiającego), bez wpływu na warunki gwarancji i naprawy urządzenia.
Wymagania dodatkowe	Oferowany sprzęt musi być fabrycznie nowy, nieużywany, sprawny oraz posiadać karty gwarancyjne lub zapewniać dostęp do dokumentacji gwarancyjnej umożliwiającej zapoznanie się z warunkami gwarancji. Sprzęt musi spełniać wymagania techniczne i być zgodny z jego przeznaczeniem zgodnie z przepisami prawa oraz zasadami techniczno-gospodarczymi. Oferowany sprzęt musi być wolny od wad technicznych, kompletny, zgodny z obowiązującymi przepisami oraz normami. Musi być dostarczony w oryginalnych opakowaniach producenta, zaopatrzonych w etykiety identyfikacyjne zawierające nazwę produktu, numer seryjny oraz producenta. System operacyjny musi być zainstalowany. Całość ma stanowić zestaw funkcjonalnie pełny, tzn. musi zawierać wszystkie podzespoły niezbędne do prawidłowej pracy komputera przenośnego, których Zamawiający nie precyzuje.

KRYTERIA RÓWNOWAŻNOŚCI DLA SYSTEMU OPERACYJNEGO

Informacje dotyczące licencjonowania zaoferowanego systemu operacyjnego:

1. Licencja na zaoferowany system operacyjny musi być w pełni zgodna z warunkami licencjonowania producenta oprogramowania.
2. Licencja musi być nieużywana i nieaktywowana nigdy wcześniej na innym urządzeniu.
3. Oprogramowanie musi być zainstalowane przez producenta komputera.
4. Zamawiający przewiduje możliwość zastosowania procedury sprawdzającej legalność zainstalowanego oprogramowania w momencie odbioru sprzętu (w wypadku wystąpienia wątpliwości co do jego legalności).

Parametry równoważności dla systemu operacyjnego Microsoft Windows 11 Professional PL 64-bit (bez wykorzystania jakichkolwiek emulatorów czy aplikacji):

1. Możliwość pełnej integracji z domeną Active Directory Microsoft Windows (posiadaną przez Zamawiającego) opartą na serwerach Windows Server 2025.
2. Zarządzanie poprzez Zasady Grup (GPO) Active Directory Microsoft Windows.
3. Zapewnienie pełnej zgodności z systemem operacyjnym Windows 11 Professional PL 64-bit, w zakresie działania wszystkich użytkowanych, bądź potencjalnie użytkowanych przez Zamawiającego aplikacji narzędziowych i systemowych działających pod systemem operacyjnym Windows 11 Professional PL 64-bit, w szczególności: Microsoft Office 2010, 2013, 2016, 2019, 2021, 2024 oraz Eset Endponit Security w wersji 12 i 13. Niewymagający dodatkowych nakładów finansowych ze strony Zamawiającego w celu dostosowania zaoferowanego oprogramowania do ww. systemów.

4. Wbudowany system pomocy w języku polskim.
5. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.
6. Funkcje związane z obsługą urządzeń typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.
7. Funkcjonalność rozpoznawania mowy, pozwalająca na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.
8. Możliwość dokonywania poprzez Internet bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego, mechanizmem udostępnianym przez producenta wraz z mechanizmem sprawdzającym, które z poprawek są potrzebne.
9. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
10. Wbudowana zapora sieciowa dla ochrony połączeń sieciowych. Zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i IP v6.
11. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
12. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi).
13. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której przyłączony jest komputer.
14. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę Zamawiający rozumie zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.
15. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.
16. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe.
17. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie. Praca systemu w trybie ochrony kont użytkowników.
18. Mechanizm pozwalający użytkownikowi zarejestrowanemu w systemie instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
19. 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.
20. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
21. Obsługa standardu NFC (Near Field Communication).
22. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
23. Wsparcie dla protokołu IPsec oparte na politykach – wdrażanie IPsec oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
24. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
25. Mechanizmy uwierzytelniania w oparciu o:
    a) Login i hasło.
    b) Karty z certyfikatami (smartcard).
    c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
    d) Wirtualną tożsamość użytkownika potwierdzaną za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza

prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu. Mechanizm musi być ze specyfikacją FIDO.

26. Mechanizmy wieloskładnikowego uwierzytelniania.
27. Wsparcie dla uwierzytelniania na bazie Kerberos v.5.
28. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu.
29. Wsparcie dla algorytmów Suite B (RFC 4869).
30. Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji Zamawiającego.
31. Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk.
32. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku.
33. Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym.
34. Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny.
35. Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol 2.0.
36. Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji Zamawiającego.
37. Możliwość konfiguracji trybu „kioskowego" dającego dostęp tylko do wybranych aplikacji i funkcji systemu.
38. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v.2 (IKEv2) dla warstwy transportowej IPsec.
39. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.
40. Wsparcie dla środowisk .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
41. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
42. Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji Zamawiającego bez konieczności tworzenia obrazu instalacyjnego (provisioning).
43. Oprogramowanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową.
44. Oprogramowanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.
45. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
46. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi, tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
47. Udostępnianie wbudowanego modemu.
48. Oprogramowanie dla tworzenia kopii zapasowych (Backup): automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
49. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
50. 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.).
51. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).

52. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie maszyn wirtualnych.
53. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.
54. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
55. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.
56. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
57. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
58. Interfejs graficzny użytkownika pozwalający na obsługę:
    a) klasyczną przy pomocy klawiatury i myszy,
    b) dotykową, umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych.
59. Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym polskim i angielskim.
60. Zlokalizowane w języku polskim co najmniej następujące elementy: menu, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe.
61. Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje.

Kryteria równoważności w zakresie systemu operacyjnego – informacje dodatkowe:

1. Przedmiot zamówienia w zakresie systemu operacyjnego został opisany przez Zamawiającego przez wskazanie znaku towarowego, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę z uwagi na fakt, że Zamawiający nie może opisać przedmiotu zamówienia w tym zakresie w wystarczająco precyzyjny i zrozumiały sposób, a wskazaniu temu towarzyszą wyrazy „lub równoważny".
2. W opisie przedmiotu zamówienia Zamawiający wskazał kryteria stosowane w celu oceny równoważności. W przypadku zaoferowania przez Wykonawcę rozwiązania (oprogramowania) równoważnego, na Wykonawcy spoczywa obowiązek wykazania równoważności, w sposób umożliwiający Zamawiającemu weryfikację spełniania przez to rozwiązanie (oprogramowanie) równoważne wszystkich wskazanych przez Zamawiającego kryteriów równoważności.

KRYTERIA RÓWNOWAŻNOŚCI DLA OPROGRAMOWANIA BIUROWEGO

Informacje dotyczące licencjonowania zaoferowanego oprogramowania biurowego:

1. Licencja na zaoferowane oprogramowanie biurowe musi być w pełni zgodna z warunkami licencjonowania producenta oprogramowania.
2. Licencja musi być nieużywana i nieaktywowana nigdy wcześniej na innym urządzeniu.
3. Zamawiający sam dokona instalacji oprogramowania biurowego. Wykonawca dostarczy jedynie wymagane klucze licencyjne oraz wskaże skąd Zamawiający może pobrać pliki instalacyjne.
4. Zamawiający przewiduje możliwość zastosowania procedury sprawdzającej legalność oferowanego oprogramowania biurowego w momencie odbioru sprzętu (w wypadku wystąpienia wątpliwości co do jego legalności).

Parametry równoważności dla oprogramowania biurowego Microsoft Office 2024 Professional Plus (bez wykorzystania jakichkolwiek emulatorów czy aplikacji):

1. Oprogramowanie biurowe musi umożliwiać pracę w trybie offline (brak konieczności podłączenia do Internetu) wraz z możliwością zapisania dokumentów na lokalnym dysku komputera.
2. Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych tylko o rozwiązania chmurowe oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu.
3. Oprogramowanie biurowe powinno być w najnowszej wersji dostępnej na rynku.
4. Dla oprogramowania musi być publicznie znany cykl życia przedstawiony przez producenta oprogramowania i dotyczący rozwoju wsparcia technicznego – w szczególności w zakresie bezpieczeństwa. Wymagane jest prawo do instalacji aktualizacji i poprawek do danej wersji oprogramowania, udostępnianych bezpłatnie przez producenta na jego stronie internetowej w okresie co najmniej 5 lat.
5. Zamawiający wymaga, aby wszystkie elementy oprogramowania biurowego oraz jego licencja pochodziły od tego samego producenta.
6. Oprogramowanie biurowe musi zawierać w pakiecie edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji, system obsługi relacyjnych baz danych, program do obsługi poczty elektronicznej.
7. Aplikacja do tworzenia prezentacji powinna umożliwiać udostępnianie prezentacji przy użyciu przeglądarki internetowej bez potrzeby instalowania dodatkowych elementów ani konfigurowania.
8. Do każdej prezentacji można dodać wciągające wideo, aby zwrócić uwagę odbiorców. Nagrania wideo można wstawiać bezpośrednio w programie, a następnie dostosowywać je, przycinać lub oznaczać najważniejsze sceny w nagraniu zakładkami, aby zwrócić na nie szczególną uwagę. Wstawiane nagrania są domyślnie osadzone, dzięki czemu nie trzeba zarządzać dodatkowymi plikami wideo.
9. Pliki programów edytora tekstów, arkusza kalkulacyjnego i programu do tworzenia prezentacji można przechowywać online i uzyskiwać do nich dostęp, przeglądać, edytować i udostępniać innym użytkownikom.
10. Wymagania odnośnie interfejsu użytkownika:
    a) Pełna polska wersja językowa interfejsu użytkownika;
    b) Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych;
    c) Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
11. 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;
    c) umożliwia wykorzystanie schematów XML;
    d) wspiera w swojej specyfikacji podpis elektroniczny.

12. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców.
13. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
14. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
15. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
    a) Edytor tekstów;
    b) Arkusz kalkulacyjny;
    c) Oprogramowanie do przygotowywania i prowadzenia prezentacji;
    d) Oprogramowanie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami);
    e) System obsługi relacyjnych baz danych.
16. 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) Sprawdzanie pisowni w języku polskim;
    i) Śledzenie zmian wprowadzonych przez użytkowników;
    j) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności;
    k) Określenie układu strony (pionowa/pozioma);
    l) Wydruk dokumentów;
    m) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną;
    n) Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, 2007,2010, 2013, 2016, 2019, 2021 i 2024 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu;
    o) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji;
17. 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, webservice);
    e) Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych.
    f) Zawierać narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych;

g) Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych;
h) Wyszukiwanie i zamianę danych;
i) Wykonywanie analiz danych przy użyciu formatowania warunkowego;
j) Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie;
k) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności;
l) Formatowanie czasu, daty i wartości finansowych z polskim formatem;
m) Zapis wielu arkuszy kalkulacyjnych w jednym pliku;
n) Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, 2007, 2010, 2013, 2019, 2021 i 2024, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń;
o) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

18. Oprogramowania do przygotowywania i prowadzenia prezentacji musi umożliwiać:
a) Przygotowywanie prezentacji multimedialnych;
b) Prezentowanie przy użyciu projektora multimedialnego;
c) Drukowanie w formacie umożliwiającym robienie notatek
d) Zapisanie jako prezentacja tylko do odczytu;
e) Nagrywanie narracji i dołączanie jej do prezentacji;
f) Opatrywanie slajdów notatkami dla prezentera;
g) Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo;
h) Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego;
i) Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym;
j) Możliwość tworzenia animacji obiektów i całych slajdów;
k) Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera;
l) Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, 2007, 2010, 2013. 2016, 2019, 2021 i 2024.

19. Oprogramowanie 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 określanie 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 użytkowników.

20. System obsługi relacyjnych baz danych musi umożliwiać tworzenie i przetwarzanie baz danych.
21. W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania.

Kryteria równoważności w zakresie oprogramowania biurowego – informacje dodatkowe:

1. Przedmiot zamówienia w zakresie oprogramowania biurowego został opisany przez Zamawiającego przez wskazanie znaku towarowego, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę z uwagi na fakt, że Zamawiający nie może opisać przedmiotu zamówienia w tym zakresie w wystarczająco precyzyjny i zrozumiały sposób, a wskazaniu temu towarzyszą wyrazy „lub równoważny".
2. W opisie przedmiotu zamówienia Zamawiający wskazał kryteria stosowane w celu oceny równoważności. W przypadku zaoferowania przez Wykonawcę rozwiązania (oprogramowania) równoważnego, na Wykonawcy spoczywa obowiązek wykazania równoważności, w sposób umożliwiający Zamawiającemu weryfikację spełniania przez to rozwiązanie (oprogramowanie) równoważne wszystkich wskazanych przez Zamawiającego kryteriów równoważności.

MINIMALNE PARAMETRY TECHNICZNO-JAKOŚCIOWE URZĄDZEŃ PERYFERYJNYCH

Monitor komputerowy

- Matryca IPS, matowa, podświetlenie LED.
- Ekran płaski, przekątna ekranu minimum 23,8".
- Rozdzielczość ekranu min. 1920x1080 (Full HD), format 16:9.
- Częstotliwość odświeżania 60Hz.
- Złącza: HDMI, DisplayPort, audio.
- Wbudowane głośniki.
- Regulacja wysokości ekranu oraz regulacja kąta pochylenia ekranu.
- Redukcja migotania, filtr światła niebieskiego.
- Dołączone przewody: HDMI, DisplayPort, zasilający.
- Kolor wiodący czarny.
- Gwarancja producenta 36 miesięcy.

Urządzenie wielofunkcyjne laserowe monochromatyczne

- Urządzenie wielofunkcyjne: drukarka, kopiarka, skaner.
- Przeznaczenie do pracy biurowej.
- Technologia druku: laserowa, monochromatyczna.
- Automatyczny druk dwustronny.
- Automatyczny podajnik dokumentów skanera (ADF).
- Standardowy podajnik papieru na 250 arkuszy (kaseta), podajnik uniwersalny (tacka) na 100 arkuszy, automatyczny podajnik dokumentów skanera (ADF) na 50 arkuszy.

- Obsługiwane typy nośników: Podajnik standardowy (kaseta) – papier standardowy, makulaturowy, cienki i gruby, o gramaturze 60-163 g/m^2; Podajnik uniwersalny – papier standardowy, makulaturowy, cienki i gruby, o gramaturze 60-230 g/m^2; Podajnik dokumentów skanera (ADF) - papier standardowy i makulaturowy, o gramaturze 64-90 g/m^2.
- Formaty obsługiwanego papieru: A4, A5, A6, B5, Letter.
- Szybkość druku: A4 jednostronnie – do 48 str./minutę, A4 dwustronnie – do 24 str./minutę.
- Rozdzielczość drukowania do 1200x1200 dpi.
- Szybkość kopiowania A4 jednostronnego do 48 str./min.
- Rozdzielczość kopiowania do 1200x600 dpi.
- Szybkość skanowania do 20 obrazów na minutę.
- Rozdzielczość skanowania: z szyby do 1200x1200 dpi, z ADF do 600x600 dpi.
- Skanowanie bezpośrednio do komputera, skanowanie do pamięci USB, do wiadomości e-mail, skanowanie do folderu sieciowego (SMB).
- Wbudowany wyświetlacz do zarządzania funkcjami urządzenia.
- Wbudowana pamięć 512MB.
- Interfejs komunikacyjny USB 2.0 oraz interfejs sieci przewodowej RJ-45 Gigabit Ethernet.
- Kompatybilność z systemem operacyjnym Windows 11.
- Dołączony standardowy wkład z tonerem dedykowany dla urządzenia (nie jest dopuszczalny toner startowy).
- Gwarancja producenta 24 miesiące.
- Sprzęt musi być fabrycznie nowy, sprawny, wolny od wad i nie może być wcześniej używany.

Drukarka laserowa monochromatyczna

- Przeznaczenie do pracy biurowej.
- Technologia druku: laserowa, monochromatyczna.
- Automatyczny druk dwustronny.
- Standardowy podajnik papieru na 250 arkuszy (kaseta), podajnik uniwersalny (tacka) na 100 arkuszy.
- Obsługiwane typy nośników: Podajnik standardowy (kaseta) – papier standardowy, makulaturowy, o gramaturze 60-163 g/m^2; Podajnik uniwersalny – papier standardowy, makulaturowy, cienki i gruby, o gramaturze 60-230 g/m^2.
- Formaty obsługiwanego papieru: A4, A5, A6, Letter.
- Szybkość druku: A4 jednostronnie – do 48 str./minutę, A4 dwustronnie – do 24 str./minutę.
- Rozdzielczość drukowania do 1200x1200 dpi.
- Wbudowany wyświetlacz do zarządzania funkcjami urządzenia.
- Wbudowana pamięć 256MB.
- Interfejs komunikacyjny USB 2.0 oraz interfejs sieci przewodowej RJ-45 Gigabit Ethernet.
- Kompatybilność z systemem operacyjnym Windows 11.
- Dołączony standardowy wkład z tonerem dedykowany dla urządzenia (nie jest dopuszczalny toner startowy).
- Gwarancja producenta 24 miesiące.
- Sprzęt musi być fabrycznie nowy, sprawny, wolny od wad i nie może być wcześniej używany.

Część II – Dostawa licencji na oprogramowanie antywirusowe Eset Protect Entry lub równoważnego

W ramach części II Wykonawca ma dostarczyć Zamawiającemu **licencję na oprogramowanie antywirusowe ESET PROTECT Entry na 230 stanowisk do ochrony stacji roboczych i serwerów lub oprogramowanie antywirusowe równoważne**. Kryteria równoważności zostały określone poniżej.

Zamawiający posiada obecnie licencję na oprogramowanie antywirusowe ESET PROTECT Entry na 230 stanowisk. Licencja ważna jest do dnia 31.12.2026 roku. **Zamówieniem objęte jest odnowienie posiadanej licencji na 230 stanowisk na 2027 rok (na tym samym kluczu licencyjnym). W przypadku zaoferowania oprogramowania antywirusowego równoważnego zamówieniem objęty jest zakup nowej licencji na 230 stanowisk na 2027 rok.**

W przypadku zaoferowania oprogramowania antywirusowego równoważnego Wykonawca oprócz dostawy licencji musi dodatkowo na swój koszt dokonać pełnej migracji do zaoferowanego oprogramowania antywirusowego równoważnego, w tym wykonać:

- Odinstalowanie obecnie posiadanego oprogramowania antywirusowego Zamawiającego na wszystkich stacjach roboczych i serwerach Zamawiającego we wszystkich lokalizacjach OHP w województwie podlaskim (Białystok, Augustów, Grajewo, Kolno, Łomża, Suwałki, Wasilków, Zambrów) – około 230 stanowisk.
- Odinstalowanie oprogramowania do komunikacji z obecną konsolą do zarządzania oprogramowaniem antywirusowym (tzw. agent) na wszystkich stacjach roboczych i serwerach Zamawiającego we wszystkich lokalizacjach OHP w województwie podlaskim (Białystok, Augustów, Grajewo, Kolno, Łomża, Suwałki, Wasilków, Zambrów) – około 230 stanowisk.
- Zainstalowanie zaoferowanego oprogramowania antywirusowego równoważnego na wszystkich stacjach roboczych i serwerach Zamawiającego we wszystkich lokalizacjach OHP w województwie podlaskim (Białystok, Augustów, Grajewo, Kolno, Łomża, Suwałki, Wasilków, Zambrów) – około 230 stanowisk.
- Zainstalowanie oprogramowania do komunikacji z nową konsolą zarządzania oprogramowaniem antywirusowym równoważnym (tzw. agent) na wszystkich stacjach roboczych i serwerach Zamawiającego we wszystkich lokalizacjach OHP w województwie podlaskim (Białystok, Augustów, Grajewo, Kolno, Łomża, Suwałki, Wasilków, Zambrów) – około 230 stanowisk.
- Uruchomienie i wdrożenie nowej zdalnej konsoli do zarządzania oprogramowaniem antywirusowym równoważnym. W ramach wdrożenia nowej konsoli należy m.in. dodać do konsoli wszystkie chronione stacje robocze i serwery, przypisać je odpowiednio do struktury organizacyjnej Zamawiającego, opisać wszystkie stanowiska oraz otagować je zgodnie z wytycznymi Zamawiającego. Należy również skonfigurować i wdrożyć obecnie posiadane przez Zamawiającego polityki bezpieczeństwa oraz przypisać te polityki do poszczególnych stacji roboczych i serwerów zgodnie z wytycznymi Zamawiającego.
- Odinstalowywanie oraz instalowanie oprogramowania musi odbywać się w siedzibie Zamawiającego w poszczególnych lokalizacjach wymienionych powyżej. Odinstalowywania oraz instalowania oprogramowania może dokonać wyłącznie pracownik Wykonawcy posiadający odpowiednią wiedzę i doświadczenie w tym zakresie, pod nadzorem Administratora Systemów Informatycznych Podlaskiej Wojewódzkiej Komendy OHP. Zamawiający może zażądać od Wykonawcy przedłożenia dokumentów potwierdzających wiedzę i doświadczenie pracowników Wykonawcy, którzy będą dokonywać wyżej wymienionej migracji oraz konfiguracji oprogramowania. Ze względów bezpieczeństwa oraz ze względu na

obowiązującą u Zamawiającego „Politykę ochrony danych”, Zamawiający nie dopuszcza możliwości zdalnego odinstalowywania oraz instalowania oprogramowania antywirusowego równoważnego przez Wykonawcę.

- Wykonawca musi przeprowadzić szkolenie dla min. 2 pracowników Zamawiającego w zakresie funkcjonalności i obsługi zaoferowanego oprogramowania antywirusowego równoważnego oraz zdalnej konsoli do zarządzania oprogramowaniem antywirusowym równoważnym. Szkolenie może być przeprowadzone stacjonarnie lub zdalnie, czas trwania szkolenia to minimum 8 godzin. Szkolenie musi zostać przeprowadzone przed dokonaniem migracji do nowego oprogramowania antywirusowego równoważnego.
- Migracja do nowego oprogramowania antywirusowego równoważnego musi zostać przeprowadzona w ciągu 14 dni roboczych oraz przed terminem zakończenia licencji na obecnie posiadane przez Zamawiającego oprogramowanie antywirusowe.

Zakupiona licencja ma być ważna i aktywna od dnia 01.01.2027 do dnia 31.12.2027 roku. Wykonawca dostarczy jeden certyfikat z kluczem licencyjnym na oprogramowanie ESET PROTECT Entry lub na oprogramowanie antywirusowe równoważne na 230 stanowisk ważny do 31.12.2027 roku.

Licencja powinna w czasie jej obowiązywania zapewniać: wsparcie techniczne producenta oprogramowania, dostęp do aktualizacji sygnatur wirusów i oprogramowania. Zamawiający dopuszcza dostarczenie licencji w postaci elektronicznej. Zamawiający dopuszcza dostarczenie oprogramowania i certyfikatu w postaci elektronicznej.

KRYTERIA RÓWNOWAŻNOŚCI W ZAKRESIE OPROGRAMOWANIA ANTYWIRUSOWEGO

Informacje dotyczące licencjonowania zaoferowanego oprogramowania antywirusowego:

1. Licencja na zaoferowane oprogramowanie antywirusowe musi być w pełni zgodna z warunkami licencjonowania producenta oprogramowania.
2. Licencja musi być nieużywana i nieaktywowana nigdy wcześniej.
3. Wykonawca dostarczy wymagane klucze licencyjne.
4. Zamawiający przewiduje możliwość zastosowania procedury sprawdzającej legalność oferowanego oprogramowania antywirusowego (w wypadku wystąpienia wątpliwości co do jego legalności).

Parametry równoważności dla oprogramowania antywirusowego ESET PROTECT ENTRY:

Administracja zdalna (konsola do zarzadzania)

1. Konsola centralnego zarządzania musi być dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS).
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu przeglądarki internetowej.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiającą co najmniej:
   a) pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania,

b) pośredniczenie w komunikacji pomiędzy stacją zarządzaną, a serwerami aktualizacjami producenta,
c) buforowanie ruchu HTTPS.

6. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej.
8. Uwierzytelnianie dwuskładnikowe musi być realizowane co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android:
   a) Google Authenticator,
   b) Microsoft Authenticator,
   c) Authy.
   d) aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. 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:
    a) adresy sieciowe IP,
    b) aktywne zagrożenia,
    c) stan funkcjonowania oraz ochrony,
    d) wersja systemu operacyjnego,
    e) podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:
    a) wyrażenie CRON,
    b) codziennie,
    c) cotygodniowo,
    d) co miesiąc,
    e) co rok,
    f) po wystąpieniu nowego zdarzenia,
    g) po automatycznym umieszczeniu hosta w grupie dynamicznej.
13. Konsola centralnego zarządzania musi być dostępna co najmniej w językach polskim oraz angielskim.
14. Język konsoli centralnego zarządzania musi być możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania.
15. Rozwiązanie musi umożliwiać tagowanie obiektów.
16. Rozwiązanie musi posiadać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.
17. Eksport danych musi być możliwy w co najmniej następujących formatach: JSON, LEEF, CEF.

Ochrona stacji roboczych – Windows

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
6. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet.
7. Rozwiązanie musi zapewniać możliwość skanowania w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   a) całego dysku,
   b) wybranych katalogów,
   c) pojedynczych plików,
   d) plików spakowanych oraz skompresowanych,
   e) dysków sieciowych,
   f) dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
   a) wybranych plików,
   b) wybranych procesów,
   c) wybranych lokalizacji,
   d) wybranych rozszerzeń,
   e) nazwy wykrycia,
   f) sumy kontrolnej (SHA1).
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
    a) sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego,
    b) konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników,
    c) konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
12. 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).
13. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
14. 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
15. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
    a) Typ urządzenia – w tym: pamięci masowe, optyczne pamięci masowe, pamięci masowe Firewire, urządzenia do tworzenia obrazów, drukarki USB, urządzenia Bluetooth, czytniki kart inteligentnych, modemy, porty LPT/COM, urządzenia przenośne.
    b) Parametry urządzenia – w tym: numer seryjny, producent, model.
    c) Typ dostępu – w tym: brak możliwości zapisu, pełen dostęp, ostrzeżenie użytkownika, brak dostępu.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    a) Tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika.
    b) Tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie.

c) Tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika.
d) 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.
e) Tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji:
    a) Funkcja generująca taki raport ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
    b) Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone, pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.
    c) Raport musi posiadać co najmniej:
        - listę zainstalowanych aplikacji,
        - listę usług systemowych,
        - informacje o systemie operacyjnym i sprzęcie,
        - listę aktywnych procesów i połączeń sieciowych,
        - harmonogram systemu operacyjnego,
        - szczegóły pliku hosts,
        - informacje o sterownikach.
18. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu
    a) antywirus,
    b) zapora osobista
    c) sandbox,
    d) antyspyware,
    e) metody heurystyczne.
19. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
20. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę:
    a) Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
    b) Ochrona musi być realizowana w oparciu o co najmniej:
        - globalna czarna lista RBL,
        - czarna lista użytkownika,
        - biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.
21. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
    a) Ochrona przed anomaliami sieciowymi, w tym co najmniej:
        - skanowanie portów TCP oraz UDP,
        - wykrywanie duplikacji adresu IP,
        - atak zatruwania ARP,
        - nieprawidłowa długość pakietu TCP oraz UDP.
    b) Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów: RDP, SMB, My SQL, MS SQL.

c) Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

22. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego:
    a) Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
    b) Zapora osobista musi posiadać co najmniej cztery tryby pracy:
        - tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
        - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
        - tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
        - tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
    c) Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.
23. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego:
    a) Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
    b) Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
    c) W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.
24. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta:
    a) Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.
    b) Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej treść komunikatu i obraz.

Ochrona serwerów – Windows Server

1. Rozwiązanie musi wspierać systemy w tym co najmniej:
    a) Microsoft Windows Server 2016,
    b) Microsoft Windows Server 2019,
    c) Microsoft Windows Server 2022,
    d) Microsoft Windows Server 2025.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. 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.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:

a) Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
b) Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
c) Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   a) całego dysku,
   b) wybranych katalogów,
   c) pojedynczych plików,
   d) plików spakowanych oraz skompresowanych,
   e) dysków sieciowych,
   f) dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
   a) wybranych plików,
   b) wybranych procesów,
   c) wybranych lokalizacji,
   d) wybranych rozszerzeń,
   e) nazwy wykrycia,
   f) sumy kontrolnej (SHA1).
11. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
   a) Tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika.
   b) Tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie.
   c) Tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika.
   d) 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.
   e) Tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji:
   a) Funkcja generująca taki raport ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
   b) Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.
   c) Raport musi posiadać co najmniej:
      - listę zainstalowanych aplikacji,
      - listę usług systemowych,
      - informacje o systemie operacyjnym i sprzęcie,
      - listę aktywnych procesów i połączeń sieciowych,
      - harmonogram systemu operacyjnego,
      - szczegóły pliku hosts,
      - informacje o sterowników.

14. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu:
    a) antywirus,
    b) zapora osobista,
    c) sandbox,
    d) antyspyware,
    e) metody heurystyczne.
15. Rozwiązanie musi posiadać funkcjonalność skanowania systemów wirtualnych w trybie online oraz offline w środowisku Hyper-V.
16. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
    a) typ urządzenia – w tym: pamięci masowe, optyczne pamięci masowe, pamięci masowe Firewire, urządzenia do tworzenia obrazów, drukarki USB, urządzenia Bluetooth, czytniki kart inteligentnych, modemy, porty LPT/COM, urządzenia przenośne.
    b) parametry urządzenia – w tym: numer seryjny, producent, model.
    c) typ dostępu – w tym: brak możliwości zapisu, pełen dostęp, ostrzeżenie użytkownika, brak dostępu.
18. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:
    a) MS SQL,
    b) Active Directory,
    c) IIS,
    d) Sysvol,
    e) DNS,
    f) DHCP,
    g) Hyper-V,
    h) Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.
19. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
    a) Ochrona przed anomaliami sieciowymi, w tym co najmniej:
        - skanowanie portów TCP oraz UDP,
        - wykrywanie duplikacji adresu IP,
        - atak zatruwania ARP,
        - nieprawidłowa długość pakietu TCP oraz UDP.
    b) Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów: RDP, SMB, My SQL, MS SQL.
    c) Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
20. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego:
    a) Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
    b) Zapora osobista musi posiadać co najmniej cztery tryby pracy:
        - tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
        - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
        - tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

- tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.

c) Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

Mobile Device Management (MDM) – zdalne zarzadzanie urządzeniami mobilnymi

1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi i administrowania bezpieczeństwem urządzeń mobilnych.
2. MDM musi pochodzić od tego samego producenta co konsola centralnego zarządzania.
3. MDM musi umożliwiać rejestrację oraz zarządzanie urządzeniami mobilnymi z systemami Android i iOS.
4. MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
   a) usunięcie zawartości urządzenia,
   b) przywrócenie urządzenia do ustawień fabrycznych,
   c) zablokowanie urządzenia,
   d) uruchomienie sygnału dźwiękowego,
   e) lokalizację GPS,
   f) resetowanie hasła blokady ekranu.
5. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
6. MDM musi umożliwiać co najmniej:
   a) Dla systemów iOS:
      - konfigurację kont e-mail,
      - konfigurację połączeń VPN,
      - Konfigurację połączeń Wi-Fi,
      - Konfigurację listy certyfikatów,
      - możliwość uruchomienia trybu jednej aplikacji.
   b) Dla systemów Android:
      - blokadę wykonywania połączeń,
      - blokadę konfiguracji sieci Wi-Fi,
      - blokadę konfiguracji tuneli VPN,
      - zarządzenie aktualizacjami sytemu operacyjnego,
      - blokadę zmiany tapety urządzenia.

Ochrona urządzeń mobilnych z systemem Android

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania:
   a) Inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.
   b) Dokładne – skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej:
   a) złożoność kodu blokady ekranu – w tym: wzór, PIN, hasło,
   b) przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu,
   c) zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu.

5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła.
6. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.

Część III – Dostawa licencji bezpieczeństwa Unified Threat Protection (UTP) dla urządzenia FortiGate-100F

W ramach części III Wykonawca **ma odnowić Zamawiającemu licencję bezpieczeństwa Unified Threat Protection (UTP) dla urządzenia FortiGate-100F na okres 36 miesięcy**.

Zamawiający posiada aktywną licencję bezpieczeństwa na urządzenie **Fortigate-100F – numer seryjny urządzenia: FG100FTK23041391, ważną do dnia 10 grudnia 2026 roku**.

Nowa licencja bezpieczeństwa ma być aktywna **od dnia 11 grudnia 2026 roku do dnia 10 grudnia 2029 roku**.

Licencja bezpieczeństwa Unified Threat Protection (UTP) dla urządzenia FortiGate-100F musi zapewniać dostęp do następujących funkcjonalności i usług bezpieczeństwa:

1. Intrusion Prevention System (IPS) – ochrona przed atakami sieciowymi poprzez wykrywanie i blokowanie prób włamań, exploitów oraz innych zagrożeń wykorzystujących podatności systemowe
2. Advanced Malware Protection (AMP) – zaawansowana ochrona przed złośliwym oprogramowaniem, w tym ransomware, trojanami, spyware oraz innymi zagrożeniami.
3. Web Filtering – filtrowanie ruchu internetowego na podstawie kategorii stron internetowych i ich reputacji.
4. DNS Filtering – ochrona przed dostępem do złośliwych, phishingowych i niebezpiecznych domen poprzez kontrolę zapytań DNS.
5. Video Filtering – kontrola oraz filtrowanie treści multimedialnych zgodnie z polityką bezpieczeństwa organizacji.
6. Antispam Service – ochrona przed spamem, phishingiem oraz innymi niepożądanymi wiadomościami poczty elektronicznej.

Licencja ma zapewniać całodobowe wsparcie techniczne producenta, dostęp do aktualizacji oprogramowania, baz sygnatur oraz serwisu zgodnie z warunkami producenta.

Licencja musi zapewniać ciągły dostęp do aktualizacji sygnatur bezpieczeństwa, baz reputacyjnych, mechanizmów wykrywania zagrożeń oraz wsparcia technicznego przez cały okres obowiązywania subskrypcji. Oferowane oprogramowanie musi być przeznaczone dla urządzenia FortiGate 100F oraz pochodzić z autoryzowanego kanału dystrybucji producenta.

W zakresie wszystkich części Zamawiający wymaga, aby oferowane świadczenie, w tym wszystkie produkty ICT, usługi ICT oraz procesy ICT wykorzystywane do realizacji zamówienia, zarówno jako elementy główne, jak i komponenty, elementy środowiska świadczenia usługi lub rozwiązania towarzyszące, nie obejmowało:

1) produktów ICT, usług ICT lub procesów ICT wskazanych w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, stwierdzającej ich negatywny wpływ na podstawowy interes bezpieczeństwa państwa;
2) produktu ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, ani usług ICT lub procesów ICT określonych w tej decyzji.

Niespełnienie powyższego wymagania skutkuje odrzuceniem oferty odpowiednio na podstawie art. 226 ust. 1 pkt 17 albo pkt 19 ustawy Pzp.