Załącznik nr 1 do zaproszenia do szacowania

OPIS PRZEDMIOTU ZAMÓWIENIA

(opis przedmiotu szacowania)

Dostawa licencji oprogramowania do zarządzania podatnościami i poprawkami bezpieczeństwa wraz z 12-miesięcznym pakietem aktualizacji i wsparcia producenta, wdrożeniem oraz szkoleniem administratorów dla Generalnej Dyrekcji Ochrony Środowiska oraz Regionalnych Dyrekcji Ochrony Środowiska w Krakowie i w Opolu

I. WPROWADZENIE

1. Przedmiotem zamówienia jest dostawa licencji oprogramowania do zarządzania podatnościami i poprawkami bezpieczeństwa (dalej: „Oprogramowanie") dla trzech jednostek, wraz z 12-miesięcznym pakietem aktualizacji i wsparcia producenta, wdrożeniem Oprogramowania oraz szkoleniem administratorów. Wykonawca udziela 12-miesięcznej gwarancji obejmującej obsługę zgłoszeń w języku polskim.
2. Użyte w OPZ pojęcia oznaczają:
   1) **Oprogramowanie** – oprogramowanie instalowane w infrastrukturze Zamawiającego (on-premise), służące do inwentaryzacji zasobów, wykrywania podatności i błędów konfiguracji, oceny ich ryzyka oraz automatycznego wdrażania poprawek bezpieczeństwa, z poziomu jednej konsoli zarządzającej;
   2) **Instancja** – odrębna, samodzielnie działająca instalacja Oprogramowania, obejmująca serwer zarządzający, bazę danych i konsolę administracyjną, przypisana do jednej Jednostki;
   3) **Punkt końcowy** – stacja robocza, komputer przenośny, serwer fizyczny lub maszyna wirtualna objęta zarządzaniem Oprogramowania (z agentem lub skanowana bezagentowo);
   4) **Licencja bezterminowa** – licencja uprawniająca do korzystania z Oprogramowania przez czas nieoznaczony, której ważność nie zależy od utrzymywania wsparcia technicznego ani subskrypcji;
   5) **Licencja terminowa** – licencja (subskrypcja) uprawniająca do korzystania z Oprogramowania przez okres oznaczony, określony w rozdziale III ust. 3;
   6) **Pakiet producenta** – nabywane jednorazowo wraz z licencją, na okres 12 miesięcy, uprawnienie producenta do aktualizacji i nowych wersji Oprogramowania, aktualizacji baz podatności i poprawek oraz wsparcia producenta (maintenance), o którym mowa w rozdziale VII ust. 1;
   7) **Gwarancja** – obowiązki gwarancyjne Wykonawcy, w tym obsługa zgłoszeń w języku polskim, o których mowa w rozdziale VII ust. 3–6;
   8) **Jednostki** – Generalna Dyrekcja Ochrony Środowiska (GDOŚ), Regionalna Dyrekcja Ochrony Środowiska w Krakowie (RDOŚ w Krakowie) oraz Regionalna Dyrekcja Ochrony Środowiska w Opolu (RDOŚ w Opolu);
   9) **dni robocze** – dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
3. Zamówienie finansowane jest w ramach Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności (dalej: „KPO"), Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL,

infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo - Cyberbezpieczny Rząd.

4. Kody CPV: 48730000-4 Pakiety oprogramowania zabezpieczającego (główny); 72263000-6 Usługi wdrażania oprogramowania; 72261000-2 Usługi wsparcia oprogramowania; 80533100-0 Usługi szkolenia komputerowego.

II. ZAKRES I WOLUMEN PRZEDMIOTU ZAMÓWIENIA

1. Zakres zamówienia obejmuje:
   1) dostawę trzech licencji (bezterminowych albo terminowych, zgodnie z rozdziałem III) – po jednej dla każdej Jednostki – w wolumenie określonym w tabeli nr 1;
   2) dostarczenie i aktywowanie wraz z licencjami Pakietu producenta na 12 miesięcy oraz udzielenie Gwarancji na 12 miesięcy od dnia podpisania protokołu odbioru końcowego (rozdział VII);
   3) wdrożenie Oprogramowania w trzech Instancjach, w tym przygotowanie pakietu i mechanizmu dystrybucji agentów, wdrożenie pilotażowe oraz wsparcie administratorów Jednostek w masowym wdrożeniu agentów (rozdział V);
   4) szkolenie administratorów – 8 godzin zegarowych, w 2 dniach po 4 godziny, dla do 5 osób (rozdział VI);
   5) dokumentację powykonawczą w języku polskim.

Tabela nr 1. Wolumen licencji

Lp.	Jednostka i adres	Punkty końcowe łącznie	w tym serwery (min.)	Konta administratorów (min.)	Instancja
1.	Generalna Dyrekcja Ochrony Środowiska, Al. Jerozolimskie 136, 02-305 Warszawa	300	50	5	nr 1
2.	Regionalna Dyrekcja Ochrony Środowiska w Krakowie, ul. Mogilska 25, 31-542 Kraków	150	20	1	nr 2
3.	Regionalna Dyrekcja Ochrony Środowiska w Opolu, ul. Firmowa 1, 45-594 Opole	100	10	1	nr 3
RAZEM		**550**	**80**	**7**	**3**

2. Licencja serwerowa obejmuje Punkt końcowy pracujący pod kontrolą serwerowego systemu operacyjnego. Jeżeli model licencjonowania producenta nie rozróżnia licencji serwerowych i stacjonarnych, wymóg uznaje się za spełniony, gdy licencja obejmuje łącznie wskazaną liczbę Punktów końcowych, w tym wskazaną liczbę serwerów. Wymagana liczba kont administratorów oznacza możliwość jednoczesnego dostępu do konsoli Oprogramowania wskazanej liczby imiennych kont z uprawnieniami administracyjnymi (co najmniej 5 w Instancji GDOŚ i co najmniej 1 w każdej Instancji RDOŚ), bez dodatkowych opłat.
3. Zamawiający wymaga trzech niezależnych Instancji. Wymóg wynika z tego, że GDOŚ, RDOŚ w Krakowie i RDOŚ w Opolu są odrębnymi jednostkami organizacyjnymi, odrębnymi administratorami danych oraz podmiotami odpowiedzialnymi za bezpieczeństwo własnych systemów, z własnymi administratorami i sieciami lokalnymi.

Niezależne Instancje zapewniają autonomię zarządzania politykami skanowania i wdrażania poprawek, rozdzielenie uprawnień oraz izolację skutków awarii lub incydentu. Zamawiający dopuszcza rozwiązanie z jedną konsolą centralną, o ile zapewnia ono równoważną separację danych, uprawnień i działania Instancji, a awaria lub niedostępność elementu centralnego nie wstrzymuje skanowania i wdrażania poprawek w pozostałych Jednostkach.

4. Zamawiający udostępni na potrzeby każdej Instancji maszynę wirtualną wraz z licencją serwerowego systemu operacyjnego z rodziny Windows Server w wersji wspieranej przez producenta. Zamawiający zapewni ponadto: konfigurację reguł zapory sieciowej zgodnie z wykazem portów przekazanym przez Wykonawcę, skrzynkę pocztową do wysyłki powiadomień i raportów, certyfikat SSL/TLS dla konsoli oraz konta w usłudze katalogowej. Wykonawca w ofercie wskaże minimalne wymagania sprzętowe (vCPU, RAM, przestrzeń dyskowa) dla każdej Instancji przy wolumenie z tabeli nr 1.

III. MODEL LICENCJONOWANIA, KWALIFIKOWALNOŚĆ I TRWAŁOŚĆ (KPO)

1. Zamawiający dopuszcza dostarczenie Licencji bezterminowych albo Licencji terminowych. Model licencjonowania stanowi kryterium oceny ofert – zaoferowanie Licencji bezterminowej będzie dodatkowo punktowane (planowane kryteria: cena 60%, model licencjonowania 35%, polska wersja językowa interfejsu 5%). Preferencja dla Licencji bezterminowej wynika z zaleceń dotyczących realizacji projektów finansowanych z KPO oraz z obowiązku utrzymania efektów projektu w okresie trwałości bez ponoszenia obowiązkowych wydatków po okresie kwalifikowalności – Licencja bezterminowa wraz z Pakietem producenta, stanowiącym jej integralny element, zapewnia trwałe prawo do korzystania z Oprogramowania niezależnie od dalszego finansowania.
2. W przypadku Licencji bezterminowej Wykonawca zapewnia prawo do korzystania z Oprogramowania w zakresie wolumenu z tabeli nr 1 przez czas nieoznaczony, niezależnie od wygaśnięcia Pakietu producenta. Po wygaśnięciu Pakietu producenta Oprogramowanie nie może zostać zablokowane ani ograniczone w zakresie funkcjonalności dostępnych w dniu wygaśnięcia.
3. W przypadku Licencji terminowej licencja musi obejmować okres nie krótszy niż 36 miesięcy od dnia zawarcia umowy (okres trwałości projektu), wraz z dostępem do aktualizacji Oprogramowania oraz baz podatności i poprawek przez cały ten okres. Całość opłat za ten okres jest objęta ceną oferty i rozliczana w ramach wynagrodzenia; przed upływem okresu licencji Oprogramowanie nie może zostać zablokowane ani ograniczone.
4. Licencje zostaną udzielone na rzecz Zamawiającego (licencjobiorca: Skarb Państwa – Generalna Dyrekcja Ochrony Środowiska) z prawem korzystania z Instancji nr 2 i nr 3 przez RDOŚ w Krakowie i RDOŚ w Opolu, bez dodatkowych opłat i bez ograniczeń terytorialnych na terenie Rzeczypospolitej Polskiej.
5. Zamawiający wymaga, aby oferowany przedmiot zamówienia, w tym model licencjonowania, zakres dostawy, wdrożenia, konfiguracji, wsparcia i innych świadczeń niezbędnych do prawidłowego korzystania z Oprogramowania, umożliwiał pełne rozliczenie całości wynagrodzenia Wykonawcy w okresie kwalifikowalności wydatków projektu „Cyberbezpieczny Rząd”, tj. do dnia 31 grudnia 2026 r.
6. Oprogramowanie ma umożliwiać utrzymanie efektów projektu przez okres trwałości projektu, nie krótszy niż 36 miesięcy od dnia zawarcia umowy, bez konieczności ponoszenia po upływie okresu kwalifikowalności obligatoryjnych wydatków warunkujących uruchomienie, aktywację, zachowanie podstawowej funkcjonalności lub

korzystanie z licencji. Nie stanowi wydatku obligatoryjnego w tym rozumieniu opcjonalne przedłużenie Pakietu producenta (aktualizacje Oprogramowania i baz podatności).

7. W celu zapewnienia kwalifikowalności całości wydatku Pakiet producenta stanowi integralny element dostawy licencji: jest nabywany jednorazowo, za cenę jednorazową ujętą w cenie licencji, dostarczany i aktywowany w całości (na pełny okres 12 miesięcy) najpóźniej w dniu podpisania protokołu odbioru częściowego nr 1, co potwierdza dokument producenta (certyfikat licencyjny lub potwierdzenie z portalu producenta) wskazujący okres uprawnień. Pakiet producenta nie jest rozliczany okresowo i nie wymaga od Zamawiającego żadnych dalszych płatności ani odbiorów po dniu odbioru końcowego.
8. Obowiązki Wykonawcy wykonywane po odbiorze końcowym (rozdział VII ust. 3–6) mają charakter gwarancyjny – stanowią element należytego wykonania dostawy i wdrożenia, są objęte ceną wdrożenia i nie stanowią odrębnie wycenianej ani rozliczanej usługi.
9. Oprogramowanie nie może wymagać do działania licencji ani subskrypcji podmiotów trzecich, których koszt nie jest objęty ceną oferty (w szczególności licencji komercyjnego silnika bazy danych), ani stałego połączenia z usługą chmurową producenta. Dane o zasobach i podatnościach Zamawiającego przechowywane są wyłącznie w infrastrukturze Zamawiającego; komunikacja z serwerami producenta ograniczona jest do pobierania aktualizacji, a przesyłanie danych telemetrycznych musi być możliwe do wyłączenia.

IV. MINIMALNE WYMAGANIA TECHNICZNE I FUNKCJONALNE

Parametry określone poniżej są parametrami minimalnymi. Każde wymaganie musi być spełnione przez każdą z Instancji.

1. Architektura

1.1. Instalacja serwera zarządzającego w infrastrukturze Zamawiającego (on-premise), na maszynie wirtualnej z systemem Windows Server w wersjach 2019, 2022 lub nowszych wspieranych przez producenta systemu.

1.2. Konsola administracyjna dostępna w całości przez przeglądarkę internetową (protokół HTTPS, z możliwością użycia certyfikatu Zamawiającego), bez instalacji dodatkowego oprogramowania klienckiego, obsługująca aktualne wersje przeglądarek Chrome, Edge i Firefox.

1.3. Interfejs w języku polskim lub angielskim, z poprawną obsługą polskich znaków w danych i raportach. Interfejs konsoli administracyjnej w języku polskim, dostępny bez dodatkowych opłat, stanowi kryterium oceny ofert.

1.4. Architektura agentowa umożliwiająca zarządzanie Punktami końcowymi w sieci lokalnej, w sieci WAN (lokalizacje zdalne, wydziały zamiejscowe), w strefie DMZ oraz Punktami końcowymi pracującymi poza siecią Zamawiającego (praca zdalna) – w tym skanowanie i wdrażanie poprawek przez Internet bez konieczności zestawiania połączenia VPN, z szyfrowaniem komunikacji agent–serwer. Elementy niezbędne do realizacji tej funkcji (np. serwer bramy komunikacyjnej) są objęte ceną oferty.

1.5. Możliwość instalacji serwerów dystrybucyjnych lub równoważnych mechanizmów (np. lokalny cache, ograniczanie przepustowości) w celu optymalizacji obciążenia łączy podczas dystrybucji poprawek.

1.6. Możliwość skanowania bezagentowego co najmniej urządzeń, na których nie jest możliwa instalacja agenta (wykrywanie w sieci i inwentaryzacja).

2. Baza danych

2.1. Oprogramowanie wykorzystuje relacyjną bazę danych dostarczaną wraz z instalatorem Oprogramowania albo bazę, do której prawo korzystania przez cały okres licencji jest objęte ceną oferty.

2.2. Silnik bazy danych nie może posiadać licencyjnych ograniczeń wielkości bazy danych, liczby rekordów ani wykorzystania zasobów serwera (CPU, RAM), które uniemożliwiałyby obsługę wolumenu z tabeli nr 1 i przechowywanie danych historycznych przez co najmniej 3 lata.

2.3. Wsparcie techniczne dla silnika bazy danych w zakresie współpracy z Oprogramowaniem świadczone jest w ramach Pakietu producenta i Gwarancji.

2.4. Wykonywanie kopii zapasowych i odtwarzanie bazy danych oraz konfiguracji z poziomu konsoli Oprogramowania lub narzędzi dostarczonych z Oprogramowaniem.

3. Bezpieczeństwo dostępu i administracja

3.1. Wbudowane uwierzytelnianie wieloskładnikowe (MFA) dla kont administracyjnych.

3.2. Integracja z usługą Active Directory Zamawiającego (uwierzytelnianie i import struktury) oraz możliwość integracji z Microsoft Entra ID, wykorzystywanym w środowisku Zamawiającego.

3.3. Model uprawnień oparty na rolach (RBAC), z co najmniej rolami: administrator, operator wdrażania poprawek, audytor (tylko odczyt), gość, z możliwością tworzenia ról niestandardowych o określonych uprawnieniach oraz ograniczenia uprawnień do wybranych grup Punktów końcowych.

3.4. Zakładanie kont użytkowników konsoli z uwierzytelnianiem lokalnym lub przez usługę katalogową.

3.5. Rejestrowanie działań administratorów (dziennik zdarzeń audytowych) z możliwością eksportu.

4. Wspierane systemy i inwentaryzacja

4.1. Wykrywanie podatności i wdrażanie poprawek co najmniej dla systemów: Windows 10 i Windows 11 (wersje wspierane przez producenta), Windows Server 2012 R2, 2016, 2019, 2022 i 2025; macOS – co najmniej trzy ostatnie wersje główne; dystrybucje Linux – co najmniej Red Hat Enterprise Linux, Ubuntu (wersje LTS), Debian, SUSE Linux Enterprise, Oracle Linux i Rocky Linux w wersjach wspieranych przez ich producentów.

4.2. Inwentaryzacja sprzętu i oprogramowania zainstalowanego na Punktach końcowych.

4.3. Rozpoznawanie Punktów końcowych w domenach Active Directory (w tym w wielu domenach) i w grupach roboczych; tworzenie statycznych i dynamicznych grup Punktów końcowych.

4.4. Zdalne czynności administracyjne: instalacja i deinstalacja oprogramowania, zamykanie i ponowne uruchamianie systemów, z harmonogramem i oknami serwisowymi.

5. Ocena podatności i konfiguracji

5.1. Automatyczne (według harmonogramu) i ręczne skanowanie podatności na podstawie brakujących poprawek, publicznie znanych podatności (CVE) i błędów konfiguracji.

5.2. Priorytetyzacja podatności z uwzględnieniem co najmniej oceny CVSS, dostępności publicznego exploita, wieku podatności, liczby podatnych Punktów końcowych oraz dostępności poprawki.

5.3. Aktualizacja bazy podatności i poprawek dostarczana przez producenta co najmniej raz na dobę w okresie Pakietu producenta.

5.4. Wykrywanie oprogramowania i systemów, dla których producent zakończył wsparcie (EOL), oraz oprogramowania wysokiego ryzyka (np. P2P, narzędzia zdalnego pulpitu), z możliwością jego zdalnej deinstalacji z poziomu konsoli.

5.5. Wykrywanie podatności typu zero-day oraz możliwość wdrożenia z poziomu konsoli skryptów lub ustawień ograniczających ryzyko ich wykorzystania do czasu wydania poprawki przez producenta.

5.6. Audyt konfiguracji bezpieczeństwa systemów operacyjnych z możliwością wdrażania bezpiecznej konfiguracji z poziomu konsoli (co najmniej: polityka haseł, ograniczenie uprawnień, ustawienia ochrony pamięci, wyłączanie przestarzałych protokołów).

5.7. Audyt konfiguracji serwerów WWW (hardening) – wykrywanie błędów konfiguracji narażających na ataki typu odmowa usługi (DoS), brute force, przejęcie sesji, clickjacking i ujawnienie kodu źródłowego, a także słabych protokołów i szyfrów SSL/TLS – wraz ze wskazaniem przyczyny, skutków i sposobu usunięcia.

5.8. Audyt otwartych portów TCP/UDP i przypisanych do nich usług oraz audyt stanu ochrony antywirusowej Punktów końcowych.

5.9. Ocena zgodności konfiguracji z co najmniej jednym uznanym zestawem wytycznych (np. CIS Benchmarks lub równoważnym), z raportem odstępstw.

6. Zarządzanie poprawkami bezpieczeństwa

6.1. Automatyczne pobieranie, testowanie i wdrażanie poprawek dla systemów operacyjnych Windows, macOS i Linux oraz dla co najmniej 300 aplikacji podmiotów trzecich, w tym przeglądarek internetowych, pakietów biurowych, czytników PDF, środowisk uruchomieniowych Java i archiwizatorów.

6.2. Mechanizm testowania i zatwierdzania poprawek na wybranej grupie testowej przed wdrożeniem produkcyjnym oraz polityki automatycznego wdrażania z harmonogramem, oknami serwisowymi i kontrolą ponownego uruchomienia.

6.3. Możliwość wycofania (deinstalacji) poprawki, o ile dopuszcza to producent poprawki.

6.4. Aktualizacja sterowników oraz oprogramowania układowego BIOS/UEFI komputerów stacjonarnych i przenośnych eksploatowanych przez Zamawiającego, w tym komputerów z BIOS/UEFI zabezpieczonym hasłem.

7. Raportowanie i integracje

7.1. Pulpity (dashboardy) i raporty predefiniowane co najmniej w zakresie: podatności, stanu wdrożenia poprawek, zgodności konfiguracji, zasobów oraz raport zarządczy.

7.2. Tworzenie raportów niestandardowych, eksport do formatów PDF, XLSX i CSV oraz automatyczna wysyłka raportów według harmonogramu.

7.3. Przesyłanie zdarzeń do systemu SIEM za pomocą protokołu syslog (lub równoważnego) oraz udostępnienie interfejsu API.

7.4. Powiadomienia e-mail oraz możliwość przekazywania zgłoszeń do systemu obsługi zgłoszeń (HelpDesk) Zamawiającego za pomocą poczty elektronicznej lub API.

V. WDROŻENIE

1. Wykonawca w terminie 5 dni roboczych od dnia zawarcia umowy przedstawi do akceptacji Zamawiającego plan wdrożenia obejmujący harmonogram, architekturę Instancji, wymagania wobec infrastruktury, konfigurację sieciową (porty, reguły zapory) oraz plan testów odbiorowych.
2. Wdrożenie obejmuje dla każdej Instancji co najmniej: instalację i konfigurację serwera zarządzającego i bazy danych; konfigurację MFA, ról i kont administratorów; integrację z Active Directory; konfigurację serwerów dystrybucyjnych lub mechanizmów równoważnych (jeżeli są wymagane) oraz komunikacji z Punktami końcowymi poza siecią Zamawiającego; przygotowanie pakietu instalacyjnego agenta i mechanizmu jego dystrybucji (np. zasady grupy GPO lub skrypt); wdrożenie pilotażowe na grupie testowej co najmniej 5 Punktów końcowych, w tym co najmniej 1 pracującym poza siecią Zamawiającego; konfigurację polityk skanowania, polityk wdrażania poprawek i okien serwisowych; konfigurację raportów i powiadomień; konfigurację przesyłania zdarzeń do SIEM; konfigurację kopii zapasowych; rejestrację licencji w portalu producenta na rzecz Zamawiającego.
3. Masowe wdrożenie agentów na pozostałych Punktach końcowych wykonują administratorzy Jednostek, na podstawie instrukcji przekazanej przez Wykonawcę. Wykonawca zapewnia zdalne wsparcie administratorów i usuwa problemy z instalacją agentów od dnia odbioru wdrożenia w danej Instancji, a po odbiorze końcowym – w ramach Gwarancji. Zakończenie masowego wdrożenia agentów nie jest warunkiem odbioru częściowego ani końcowego.
4. Prace wdrożeniowe realizowane są zdalnie, z wykorzystaniem szyfrowanego połączenia VPN uzgodnionego z Zamawiającym, a w razie potrzeby – w siedzibie Jednostki. Prace mogące wpływać na dostępność systemów prowadzone są w terminach uzgodnionych z Jednostką.
5. Po zakończeniu wdrożenia Wykonawca przeprowadzi, przy udziale przedstawicieli Jednostki, testy odbiorowe potwierdzające realizację wymagań z rozdziału IV. Pozytywny wynik testów jest warunkiem odbioru wdrożenia.
6. Wykonawca przekaże dokumentację powykonawczą w języku polskim, w wersji edytowalnej i PDF, zawierającą co najmniej: opis architektury i konfiguracji każdej Instancji, wykaz kont i ról, konfigurację polityk, procedurę wykonywania i odtwarzania kopii zapasowych, procedurę aktualizacji Oprogramowania, procedurę instalacji agenta na nowym Punkcie końcowym oraz protokoły z testów. Hasła i dane uwierzytelniające przekazywane są odrębnym, bezpiecznym kanałem.

VI. SZKOLENIE ADMINISTRATORÓW

1. Szkolenie zdalne (online), w wymiarze 8 godzin zegarowych, realizowane w 2 dniach roboczych po 4 godziny zegarowe, dla do 5 administratorów wskazanych przez Zamawiającego, prowadzone w języku polskim przez osobę posiadającą doświadczenie we wdrażaniu lub administrowaniu oferowanym Oprogramowaniem.
2. Program szkolenia obejmuje co najmniej: architekturę i instalację, dystrybucję agentów, zarządzanie podatnościami i ich priorytetyzację (CVSS, exploity), automatyzację wdrażania poprawek (Windows, macOS, Linux, aplikacje podmiotów trzecich), audyt konfiguracji i zgodności, raportowanie, kopie zapasowe i aktualizację Oprogramowania oraz zajęcia praktyczne na wdrożonym środowisku lub środowisku laboratoryjnym.

3. Wykonawca zapewnia platformę szkoleniową (o ile szkolenie nie odbywa się na platformie Zamawiającego) oraz materiały szkoleniowe w języku polskim w wersji elektronicznej i wydaje uczestnikom imienne zaświadczenia. Materiały i zaświadczenia oznacza się zgodnie z zasadami oznakowania KPO.
4. Szkolenie odbywa się po odbiorze wdrożenia, w terminie uzgodnionym z Zamawiającym.
5. Szkolenie jest usługą kształcenia zawodowego finansowaną w całości ze środków publicznych i korzysta ze zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług; Zamawiający złoży stosowne oświadczenie. Szkolenie wyceniane jest i fakturowane odrębnie od licencji i wdrożenia.

VII. PAKIET PRODUCENTA I GWARANCJA (12 MIESIĘCY)

1. Pakiet producenta, dostarczany i aktywowany wraz z licencjami na okres 12 miesięcy, obejmuje co najmniej: dostęp do nowych wersji, aktualizacji i poprawek Oprogramowania; aktualizacje baz podatności i poprawek; dostęp do portalu i bazy wiedzy producenta; wsparcie producenta Oprogramowania, realizowane bezpośrednio lub za pośrednictwem Wykonawcy jako autoryzowanego partnera.
2. Okres Pakietu producenta biegnie od dnia jego aktywacji, nie później niż od dnia podpisania protokołu odbioru częściowego nr 1, i wynosi 12 miesięcy. W przypadku Licencji terminowej uprawnienia, o których mowa w ust. 1, obejmują cały okres licencji.
3. W ramach Gwarancji, przez 12 miesięcy od dnia podpisania protokołu odbioru końcowego bez zastrzeżeń, Wykonawca zapewni:
   1) pomoc techniczną w języku polskim – telefonicznie, pocztą elektroniczną lub przez portal zgłoszeń, w dni robocze w godzinach co najmniej 8:00–16:00, wraz z pomocą zdalną;
   2) pomoc w instalacji nowych wersji Oprogramowania oraz konsultacje w zakresie konfiguracji i raportowania;
   3) co najmniej jeden zdalny przegląd każdej Instancji (stan, wydajność, kopie zapasowe, aktualność wersji) w okresie Gwarancji, zakończony raportem z rekomendacjami.
4. Wymagane czasy obsługi zgłoszeń gwarancyjnych (liczone w dni robocze, w godzinach 8:00–16:00):

Kategoria	Opis	Czas reakcji	Czas obejścia lub naprawy
Awaria krytyczna	Instancja niedostępna albo brak możliwości skanowania lub wdrażania poprawek	4 godziny	2 dni robocze
Błąd istotny	Nieprawidłowe działanie funkcji Oprogramowania, bez zatrzymania jego pracy	8 godzin	5 dni roboczych
Zgłoszenie zwykłe	Pytania, konsultacje, zgłoszenia „how-to”	2 dni robocze	10 dni roboczych

5. Czas naprawy błędu, którego usunięcie wymaga poprawki producenta, może zostać wydłużony za zgodą Zamawiającego, pod warunkiem zastosowania obejścia.
6. Gwarancja jest objęta ceną wdrożenia i nie podlega odrębnemu wynagrodzeniu ani rozliczeniu.

VIII. WYMAGANIA OGÓLNE

1. Licencje muszą pochodzić z autoryzowanego kanału dystrybucji producenta, być nowe, nieużywane i zarejestrowane na rzecz Zamawiającego. Wykonawca dołączy do oferty oświadczenie, że oferowana wersja Oprogramowania nie ma ogłoszonej daty zakończenia sprzedaży lub wsparcia (End-of-Sale/End-of-Life) przypadającej w okresie Pakietu producenta i Gwarancji.
2. Wszędzie tam, gdzie w OPZ wskazano znaki towarowe, nazwy produktów, standardy lub normy, Zamawiający dopuszcza rozwiązania równoważne, zapewniające co najmniej tę samą funkcjonalność, poziom bezpieczeństwa i zgodność ze środowiskiem Zamawiającego. Obowiązek wykazania równoważności spoczywa na Wykonawcy.
3. Wykonawca oferuje wyłącznie produkty, usługi i procesy ICT, które na dzień składania ofert nie są objęte rekomendacją, o której mowa w art. 33 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa, ani decyzją o uznaniu dostawcy za dostawcę wysokiego ryzyka. Wykonawca jednoznacznie identyfikuje oferowane Oprogramowanie (nazwa, producent, edycja i wersja).
4. Przedmiot zamówienia jest zgodny z zasadą „nie czyń znaczącej szkody” (DNSH) i nie wywiera znaczącego negatywnego wpływu na cele środowiskowe. Dostawa realizowana jest w postaci elektronicznej, bez nośników fizycznych, a wdrożenie i szkolenie – co do zasady zdalnie.
5. Wykonawca podczas wdrożenia i wykonywania Gwarancji może uzyskać dostęp do danych osobowych przetwarzanych w systemach Jednostek (np. nazwy kont użytkowników, nazwy komputerów, adresy IP). Przed rozpoczęciem prac Wykonawca zawrze umowę powierzenia przetwarzania danych osobowych z każdą Jednostką, według wzoru tej Jednostki, i zobowiąże swój personel do zachowania poufności.
6. Dokumenty przekazywane w trakcie realizacji umowy zawierające informacje o infrastrukturze Zamawiającego przekazywane są w zaszyfrowanych archiwach (AES-256), a hasło – innym kanałem komunikacji. Wykonawca nie kopiuje dokumentów Jednostek poza zasoby służbowe niezbędne do realizacji umowy i usuwa je najpóźniej z chwilą zakończenia umowy.
7. Dokumenty wytworzone przez Wykonawcę (plan wdrożenia, dokumentacja powykonawcza, materiały szkoleniowe, zaświadczenia, raporty) oznacza się zgodnie z Księgą Identyfikacji Wizualnej KPO.
8. Komunikacja, dokumentacja, szkolenie i obsługa zgłoszeń gwarancyjnych prowadzone są w języku polskim.

IX. TERMINY I DOKUMENTY ODBIOROWE

1. Termin realizacji: dostawa licencji – do 5 dni roboczych od dnia zawarcia umowy; wdrożenie i szkolenie – do 30 dni od dnia zawarcia umowy. Całość przedmiotu zamówienia, łącznie z podpisaniem protokołów odbioru częściowego i protokołu odbioru końcowego oraz wystawieniem i doręczeniem faktury, musi zostać zrealizowana nie później niż do dnia 15 grudnia 2026 r. Wykonawca zgłasza gotowość do odbioru końcowego nie później niż do dnia 4 grudnia 2026 r., tak aby możliwe było usunięcie ewentualnych zastrzeżeń przed tym terminem.
2. Odbiory częściowe dokumentowane są protokołami odbioru częściowego: nr 1 – dostawa licencji; nr 2, 3 i 4 – wdrożenie odpowiednio w Instancji GDOŚ, RDOŚ w Krakowie i RDOŚ w Opolu.

3. Warunkiem odbioru dostawy licencji jest przekazanie certyfikatów licencyjnych lub kluczy oraz potwierdzenia rejestracji licencji oraz aktywacji Pakietu producenta na pełny okres 12 miesięcy w portalu producenta na rzecz Zamawiającego.
4. Warunkiem odbioru wdrożenia w danej Instancji jest pozytywny wynik testów odbiorowych tej Instancji, w tym na Punktach końcowych pilotażowych, oraz przekazanie części dokumentacji powykonawczej dotyczącej tej Instancji.
5. Warunkiem odbioru końcowego jest podpisanie bez zastrzeżeń protokołów odbioru częściowego nr 1–4, przeprowadzenie szkolenia (lista obecności, zaświadczenia), przekazanie kompletnej dokumentacji powykonawczej oraz danych dostępowych do portalu wsparcia.

Nie jestem radcą prawnym, a dokumentacja wymaga ostatecznej akceptacji formalno-prawnej.