Zgierz dnia 28 sierpnia 2024 r.

Znak sprawy: IB.272.1.2024.AO

ZAPYTANIE OFERTOWE

I. ZAMAWIAJĄCY:

Powiat Zgierski, w imieniu którego działa Zarząd Powiatu Zgierskiego, 95-100 Zgierz, ul. Sadowa 6a. tel. 042 288 81 00, adres email: starostwo@powiat.zgierz.pl

jako realizator projektu realizowanego w ramach **Projektu grantowego pn. „Cyberbezpieczny Samorząd" realizowanego przez Powiat Zgierski,** dofinansowanego z Funduszy Europejskich na Rozwój Cyfrowy 2021 – 2027 (FERC), PRIORYTET II – Zaawansowane usługi cyfrowe Działanie 2.2 - Wzmocnienie krajowego systemu cyberbezpieczeństwa. Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0405/ FERC.02.02-CS.01-001/23/2024 w postępowaniu o wartości poniżej 130 000 PLN, bez stosowania przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605) mającym na celu udzielenie zamówienia publicznego zgodnie z zasadą konkurencyjności poprzez upublicznienie zapytania ofertowego na stronie internetowej: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/ w Bazie Konkurencyjności, zaprasza do złożenia oferty cenowej na **„Dostawę 200 szt. licencji na oprogramowanie zabezpieczające końcowe stacje komputerowe (antywirus, antyspyware, personal firewall, antyspam, filtr treści, sandboxing, rozszerzone wykrywanie i reagowanie XDR/EDR)".**

II. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Kod i nazwa według Wspólnego Słownika Zamówień:

   48730000-4 Pakiety oprogramowania zabezpieczającego
   80510000-2 Usługi szkolenia specjalistycznego

2. Przedmiotem zamówienia jest dostawa, wdrożenie oraz przeszkolenie personelu technicznego, na aktualizację (upgrade) oprogramowania zabezpieczającego końcowe stacje komputerowe - ESET PROTECT Enterprise, realizowanego w ramach Projektu grantowego pn. „Cyberbezpieczny Samorząd'' lub równoważnego zgodnie z zamieszczoną poniżej specyfikacją określającą minimalne parametry przedmiotu zamówienia:

Administracja zdalna w chmurze

1) W chmurze producenta.
2) Dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3) Zabezpieczenie za pośrednictwem protokołu SSL.
4) Mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5) Komunikacja agenta przy wykorzystaniu HTTP Proxy.
6) Zarządzanie urządzeniami mobilnymi – MDM.
7) Wymuszenie dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8) Dodanie zestawu uprawnień dla użytkowników w oparciu o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji ma możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9) 80 szablonów raportów, przygotowanych przez producenta.
10) Tworzenie grup statycznych i dynamicznych komputerów.
11) Grupy dynamiczne tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki zawierają: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12) Uruchamianie zadań automatycznie, z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych

1) Wsparcie systemów operacyjnych Windows (Windows 10/Windows 11).
2) Wsparcie architektury ARM64.
3) Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4) Wbudowana technologia do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5) Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6) Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7) Skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8) Skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9) Opcja umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10) Integracja z Intel Threat Detection Technology.

11) 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).
12) Skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13) Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Opcja wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14) Blokowanie zewnętrznych nośników danych na stacji w tym: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15) Blokowanie nośników wymiennych, bądź grup urządzeń umożliwia użytkownikowi tworzenie reguł dla podłączanych urządzeń w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16) Moduł HIPS ma 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 samoczynnie przełącza się w tryb pracy oparty na regułach,
e) tryb inteligentny, w którym powiadomienia będą wyłącznie o szczególnie podejrzanych zdarzeniach.
17) Wbudowana funkcja generująca pełny raport na temat stacji, na której zostało zainstalowane, z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18) Funkcja, generująca taki log, posiada 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19) Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
20) Tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21) Skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22) Ochrona antyspamowa dla programu pocztowego Microsoft Outlook.

23) Zapora osobista rozwiązania pracuje w jednym z czterech trybów:
a) tryb automatyczny –blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
b) tryb interaktywny – pyta się o każde nowo nawiązywane połączenie,
c) tryb oparty na regułach – blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
d) tryb uczenia się – automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator konfiguruje czas działania trybu.
24) Moduł bezpiecznej przeglądarki.
25) Przeglądarka automatycznie szyfruje wszelkie dane wprowadzane przez Użytkownika.
26) Praca w bezpiecznej przeglądarce jest wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27) Zintegrowany moduł kontroli dostępu do stron internetowych.
28) Filtrowanie adresów URL w oparciu o co 140 kategorii i podkategorii.
29) Ochrona przed zagrożeniami 0-day.
30) Na stacjach roboczych: wstrzymanie uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera

1) Wsparcie systemów Microsoft Windows Server 2012 i nowszych oraz Linux w tym: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
2) Ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3) Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4) Skanowanie dysków sieciowych typu NAS.
5) Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Opcja wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6) Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
7) Wykluczanie ze skanowania procesów.
8) Określenie typu podejrzanych plików, jakie będą przesyłane do producenta, w tym pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe funkcje dla ochrony serwerów Windows:

9) Skanowanie plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10) System zapobiegania włamaniom działający na hoście (HIPS).
11) Skanowanie magazynu Hyper-V.
12) Skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

13) Blokowanie zewnętrznych nośników danych na stacji w tym: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14) Automatyczne wykrywanie usług zainstalowanych na serwerze i tworzenie dla nich odpowiednich wyjątków.
15) Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16) Dodawanie wyjątków dla systemu IDS, w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17) Ochrona przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe funkcje dla ochrony serwerów Linux:

18) Uruchamianie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19) Lokalna konsola administracyjna nie wymaga do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20) Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, wspiera rozwiązanie Dell EMC Isilon.
21) Działa w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta zapewnia podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Szyfrowanie

1) Instalacja aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
2) Wsparcie zarządzania natywnym szyfrowaniem w systemach macOS (FileVault).
3) Autentykacja typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Opcja całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4) Szyfrowanie danych tylko na komputerach z UEFI.

Sandbox w chmurze

1) Ochrona przed zagrożeniami 0-day.
2) Wykorzystywanie do działania chmury producenta.
3) Opcja określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4) Definiowanie po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5) Definiowanie maksymalnego rozmiaru przesyłanych próbek.
6) Tworzenie listy wykluczeń określonych plików lub folderów z przesyłania.

7) Po zakończonej analizie pliku, przesyłany jest wynik analizy do wszystkich wspieranych produktów.
8) Podgląd listy plików, które zostały przesłane do analizy.
9) Analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10) Brak wymogu instalacji dodatkowego agenta na stacjach roboczych.
11) Wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator ma podgląd jakie pliki zostały wysłane do analizy oraz przez kogo.
12) Przeanalizowane pliki są odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
    a) Czysty,
    b) Podejrzany,
    c) Bardzo podejrzany,
    d) Szkodliwy.
13) W przypadku stacji roboczych opcja wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14) W przypadku serwerów pocztowych opcja wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15) Wykryte zagrożenia są przeniesione w bezpieczny obszar kwarantanny, z której można przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

Moduł EDR/XDR

1) Dostęp do konsoli centralnego zarządzania odbywa się z poziomu interfejsu WWW.
2) Wysyłanie zdarzeń do konsoli administracyjnej ESET.
3) Interfejs jest zabezpieczony za pośrednictwem protokołu SSL.
4) Wprowadzanie wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5) Wykluczenia dotyczą procesu lub procesu „rodzica”.
6) Utworzenie wykluczenia automatycznie rozwiązuje alarmy, które pasują do utworzonego wykluczenia.
7) Kryteria wykluczeń są konfigurowane w oparciu o: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8) Serwer posiada ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator może utworzyć własne reguły i edytować reguły dodane przez producenta.
9) Blokowanie plików po sumach kontrolnych. W ramach blokady można dodać komentarz oraz konfigurację wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
10) Weryfikacja uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję

produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.

11) W ramach plików wykonywalnych oraz plików DLL, opcja ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12) Weryfikacja uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Oznaczanie skryptu jako bezpieczny lub niebezpieczny.
13) W ramach przeglądania wykonanego skryptu, możliwy szczegółowy podgląd wykonanych przez skrypt czynności w formie tekstowej.
14) W ramach przeglądania wykonanego skryptu lub pliku exe, możliwa weryfikacja powiązanych zdarzeń dotyczących: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
15) Przekierowanie do konsoli zarządzającej ESET, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli ESET, możliwy podgląd informacji dotyczącychj: podzespołów zarządzanego PC (w tym: producent, model, numer seryjny, informacje o systemie, procesor, peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
16) Tagowanie obiektów.
17) Połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

3. Wykonawca w ramach realizacji zadania dostarczy vouchery na szkolenie 2 pracowników, ważne min. **12 miesięcy** od daty podpisania umowy. Szkolenia wykonywane będą przez ośrodki szkoleniowe autoryzowane przez producenta oprogramowania. Szkolenia muszą odbywać się na 3 poziomach zaawansowania, mogą odbywać się w trybie zdalnym, według poniższej specyfikacji:

    1) ESET Client & Network Security Administrator

        a. architektura i omówienie komponentów,
        b. Instalacja i aktualizacja serwera (ćwiczenie),
        c. Omówienie funkcji serwera,
        d. Zarządzanie administratorami i ich uprawnieniami (ćwiczenie),
        e. ESET Management Agent - zdalna instalacja i omówienie możliwości (ćwiczenie),
        f. Grupy statyczne i dynamiczne,
        g. Zadania klienta, serwera oraz wyzwalacze,
        h. Zdalna instalacja klienta,
        i. Typowe scenariusze (ćwiczenia),
        j. Omówienie funkcji podstawowych i zaawansowanych klienta EES,
        k. Ochrona antywirusowa,
        l. Zarządzanie aktualizacją,
        m. Polityki i dziedziczenie (ćwiczenie),
        n. ESET Bridge,

o. Zapora osobista (ćwiczenie),
p. Typowe scenariusze (ćwiczenia),
q. Moduł antyspamowy,
r. Powiadomienia,
s. Raportowanie (ćwiczenie),
t. Kontrola dostępu do stron internetowych (ćwiczenie),
u. Kontrola dostępu do urządzeń (ćwiczenie),
v. Migracja ESET PROTECT do ESET PROTECT CLOUD (ćwiczenie),
w. Rozwiązywanie problemów.

2) ESET Advanced Administration - warsztat praktyczn

a. Utworzenie konta ESET Business Account i dodanie kluczy licencyjnych.
b. Wdrożenie i konfiguracja serwera centralnego zarządzania w postaci maszyny wirtualnej.
c. Migracja agentów ESET Management Agent pomiędzy serwerami.
d. Wdrożenie i konfiguracja usługi ESET Bridge w celu replikacji agentów przy pracy zdalnej oraz w środowiskach rozproszonych.
e. Zaawansowane zarządzanie politykami.
f. ESET Full Disk Encryption – szyfrowanie.
g. ESET LiveGuard Advanced – sandboxing chmurowy.
h. Rozwiązywanie problemów.

3) ESET Inspect - Administrator XD

a. Omówienie pojęcia Extended Detection & Respond (XDR),
b. Architektura produktu ESET Inspect,
c. Wdrożenie serwera ESET Inspect (ćwiczenie),
d. Wdrożenie i konfiguracja agentów ESET Inspect (ćwiczenie),
e. Omówienie funkcji ESET Inspect,
f. Generowanie detekcji i ich analiza (ćwiczenie),
g. Reguły i automatyzacja (ćwiczenie),
h. Raportowanie, powiadomienia i zarządzanie uprawnieniami,
i. Rozwiązywanie problemów.

4. Wykonawca w ramach realizacji zadania dokona wdrożenia rozwiązania EDR/XDR – ESET Inspect dla 2 osobnych lokalizacji (2 osobne serwery) Zamawiającego, polegającego w szczególności na:
   1) Wdrożenie serwera ESET Inspect.
   2) Wdrożenie bazy danych na serwerze.
   3) Konfiguracja bazy danych MySQL.
   4) Wdrożenie konektorów ESET Inspect Connector.

5) Przygotowanie polityki połączeniowej i zaaplikowanie dla stacji końcowych z zainstalowanym konektorem.
6) Stworzenie minimalnie 3 wyjątków dla rozwiązania ESET Inspect.

5. Zamawiający posiada aktualną do dnia 31.12.2025 r. licencję na oprogramowanie **Eset Endpoint Security** w ilości 200 licencji.
6. W przypadku gdy opis przedmiotu zamówienia odnosi się do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, Zamawiający dopuszcza rozwiązania równoważne, w takim przypadku oferta nie zostanie odrzucona pod warunkiem, że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia. Jako rozwiązania równoważne, należy rozumieć rozwiązania charakteryzujące się parametrami nie gorszymi niż określone w opisie przedmiotu zamówienia. Jeżeli zamawiający dopuszcza rozwiązania równoważne, ale nie podaje minimalnych parametrów, które by tę równoważność potwierdzały - Wykonawca obowiązany jest zaoferować produkt o właściwościach zbliżonych, nadający się funkcjonalnie do zapotrzebowanego zastosowania kompatybilnego z urządzeniami już istniejącymi. Na Wykonawcy spoczywa obowiązek udowodnienia równoważności oferowanych rozwiązań oraz przedstawienie oświadczeń lub dowodów określających równoważność na etapie składania oferty. Zamawiający dopuszcza rozwiązania równoważne w stosunku do określonych w zapytaniu ofertowym i załącznikach do zapytania ofertowego, oznaczając takie wskazania lub odniesienia odpowiednio wyrazami „lub równoważny” lub „lub równoważne", pod warunkiem zapewnienia parametrów nie gorszych niż określone w opisie przedmiotu zamówienia. Rozwiązanie równoważne jest także dopuszczalne w sytuacji, gdyby wyraz „równoważny” lub „równoważne” nie znalazło się w opisie przedmiotu zamówienia
7. Równoważność polega na możliwości zaoferowania przedmiotu zamówienia o nie gorszych parametrach technicznych, konfiguracjach, wymaganiach normatywnych itp. Nazwy własne producentów materiałów i urządzeń podane w szczegółowym opisie należy rozumieć jako preferowanego typu w zakresie określenia minimalnych wymagań jakościowych. Nie są one wiążące i można dostarczyć elementy równoważne, które posiadają co najmniej takie same lub lepsze normy, parametry techniczne; jakościowe, funkcjonalne, będą tożsame tematycznie i o takim samym przeznaczeniu oraz nie obniżą określonych w opisie przedmiotu zamówienia standardów.
8. Oferowany przez Wykonawcę przedmiot zamówienia musi spełniać narzucone przepisami prawa wymagania w zakresie dopuszczenia do obrotu na terenie RP, posiadać wymaganą deklarację zgodności CE, certyfikaty / oświadczenia.
9. Licencja na oprogramowanie zostanie udzielona na okres **18 miesięcy**, liczony od dnia **08.10.2024r.**, na ten sam okres udzielane jest wsparcie oraz pomoc techniczna dystrybucji oprogramowania, świadczona w języku polskim.
10. Oprogramowanie musi pochodzi z polskiej dystrybucji i cała komunikacja z dystrybucją musi odbywać się w języku polskim.

11. Dostarczenie licencji i certyfikatu wyżej wymienionego oprogramowania odbędzie się na podstawie protokołu zdawczo-odbiorczego bez zastrzeżeń z realizacji niniejszego zamówienia.
12. Certyfikat i licencje zostaną wystawione na:
    Starostwo Powiatowe w Zgierzu, ul. Sadowa 6a, 95-100 Zgierz
13. Wykonawca dostarczy dokumenty potwierdzające udzielenie licencji drogą pocztową na adres Zamawiającego tj. 95-100 Zgierz, ul. Sadowa 6a oraz drogą mailową na adres: it@powiat.zgierz.pl

III. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCENY ICH SPEŁNIANIA

1. O realizację zamówienia mogą ubiegać się Wykonawcy/przedsiębiorcy - osoby fizyczne prowadzące działalność gospodarczą lub osoby prawne dysponujące odpowiednim potencjałem technicznym i osobami zdolnymi do wykonania zamówienia.

Ocena spełnienia tego warunku będzie na podstawie załączonego do oferty przez Wykonawcę aktualnego wypisu z odpowiedniego rejestru (CEiDG lub KRS).

2. Wykonawca nie może znajdować się w sytuacji ekonomicznej i finansowej mogącej budzić wątpliwości co do możliwości prawidłowego wykonania zamówienia tj. nie wszczęto wobec niego postępowania upadłościowego, ani nie ogłoszono upadłości, nie zalega z opłacaniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne.

Ocena spełnienia tego warunku będzie na podstawie załączonego do oferty oświadczenia Wykonawcy.

Ocena spełniania ww. warunków odbędzie się wg reguły spełnia/nie spełnia na podstawie w/w oświadczeń i dokumentów składanych w załączeniu do oferty.

IV. INFORMACJE NA TEMAT ZAKAZU POWIĄZAŃ OSOBOWYCH LUB KAPITAŁOWYCH – WYKLUCZENIE Z UDZIAŁU W POSTĘPOWANIU

1. W postępowaniu nie mogą brać udziału osoby, które powiązane są z Zamawiającym osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania pomiędzy Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związanych z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a Wykonawcą, polegające w szczególności na:
   1) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej, posiadaniu co najmniej 10% udziałów lub akcji (o ile niższy próg nie wynika z przepisów prawa), pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,

2) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli, albo pozostawania we wspólnym pożyciu, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych.
3) Pozostawaniu w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub zależności w związku z postępowaniem o udzielenie zamówienia.

2. Zgodnie z art. 7 ust. 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego z postępowania o udzielenie zamówienia publicznego lub z konkursu zamawiający wyklucza:
   1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 w/w ustawy;
   2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 w/w ustawy;
   3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z 29 września 1994 r. o rachunkowości jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 w/w ustawy. Wykluczenie następuje na okres trwania okoliczności określonych w ust. 1 art. 7 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.
3. W związku z powyższym Wykonawca jest zobowiązany do złożenia oświadczenia stanowiącego załącznik nr 2 do zapytania. Wykonawcy, którzy nie złożą ww. oświadczenia zostaną odrzuceni.

V. KRYTERIA OCENY OFERTY. INFORMACJA O WAGACH PUNKTOWYCH PRZYPISANYCH DO POSZCZEGÓLNYCH KRYTERIÓW OCENY OFERT. OPIS SPOSOBU PRZYZNAWANIA PUNKTACJI ZA SPEŁNIENIE DANEGO KRYTERIUM OCENY OFERT:

1. Zamawiający oceni i porówna jedynie oferty, które nie zostaną odrzucone przez Zamawiającego.

2. Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierować kryterium najniższej ceny o wadze 100% (100 pkt.).
3. Punktacja przyznawana ofertom liczona będzie z dokładnością do dwóch miejsc po przecinku, zgodnie z zasadami arytmetyki.
4. Cena ofertowa brutto musi uwzględniać wszelkie koszty jakie Wykonawca poniesie w związku z realizacją przedmiotu zamówienia.
5. Zamawiający przy obliczaniu punktów będzie posługiwał się wzorem:

Wzór obliczenia ceny:

$$Lp = Cn / Cb \times 100{,}00$$

Lp – liczba punktów

Cn – Cena najniższa z zaoferowanych

Cb – Cena badanej oferty

6. Zamawiający dokona obliczenia punktów dla każdej części osobno.
7. W toku badania i oceny ofert Zamawiający może żądać od Wykonawcy wyjaśnień dotyczących treści złożonej oferty, w tym zaoferowanej ceny.
8. O wyborze najkorzystniejszej oceny decyduje największa liczba uzyskanych punktów.

VI. OPIS SPOSOBU OBLICZANIA CENY

1. Wykonawca określa cenę realizacji zamówienia poprzez wskazanie w formularzu ofertowym sporządzonym wg wzoru stanowiącego załącznik nr 1 do niniejszego zapytania ofertowego, łącznej ceny ofertowej brutto za realizację całości przedmiotu zamówienia.
2. Łączna cena ofertowa brutto musi uwzględniać wszystkie koszty związane z realizacją przedmiotu zamówienia.
3. Ceny muszą być: podane i wyliczone w zaokrągleniu do dwóch miejsc po przecinku (zasada zaokrąglenia – poniżej 5 należy końcówkę pominąć, powyżej i równe 5 należy zaokrąglić w górę).
4. Cena oferty winna być wyrażona w złotych polskich (PLN).
5. Cena za wykonanie zamówienia jest ceną ryczałtową. Ofertowa cena powinna obejmować wynagrodzenie za wszystkie obowiązki przyszłego Wykonawcy, niezbędne do zrealizowania zamówienia.
6. Zamawiający wymaga podania ceny z podatkiem VAT (brutto) – za całość zamówienia (cena ryczałtowa) oraz kwoty podatku VAT.
7. Jeżeli Wykonawca składa ofertę, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi

przepisami. Wykonawca, składając ofertę, informuje zamawiającego, czy wybór oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku. W takim przypadku Wykonawca zobowiązany jest wskazać w formularzu oferty, że cena nie zawiera podatku VAT.

8. Zamawiający poprawi oczywiste omyłki pisarskie, oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek.
9. W szczególności Zamawiający poprawi:
   1) błędne obliczenie prawidłowo podanej przez Wykonawcę stawki podatku VAT,
   2) błędne zsumowanie w ofercie wartości netto,
   3) błędne zsumowanie w ofercie wartości brutto,
10. Zamawiający w przypadku, gdy nie będzie mógł skorzystać z ww. zasad poprawy omyłek rachunkowych będzie kierował się następującym sposobem poprawienia „oczywistej omyłki rachunkowej": błąd popełniony przez Wykonawcę w obliczeniu ceny, który polega na uzyskaniu nieprawidłowego wyniku działania arytmetycznego, przy założeniu, że składniki działania są prawidłowe, i który można jednoznacznie poprawić, zostanie poprawiony z zastosowaniem powszechnie znanych reguł arytmetycznych.

VII. TERMIN REALIZACJI ZAMÓWIENIA

Całość zamówienia należy wykonać w terminie 30 dni od dnia zawarcia umowy w sprawie udzielenia zamówienia publicznego.

VIII. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

1. Wykonawca może złożyć tylko jedną ofertę. Istnieje możliwość wycofania oferty po uprzednim złożeniu stosownego oświadczenia.
2. Oferta powinna być czytelna i złożona w języku polskim.
3. Oferta musi być sporządzona pod rygorem nieważności w formie elektronicznej (w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym) albo w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym, w języku polskim.
4. Do oferty należy dołączyć:

   1) wypełniony pismem ręcznym lub komputerowym i podpisany przez osobę reprezentującą Wykonawcę Formularz oferty (stanowiący załącznik nr 1 do Zapytania Ofertowego),

   2) czytelnie wypełnione pismem ręcznym lub komputerowym i podpisane przez osobę reprezentującą Wykonawcę oświadczenie o spełnieniu warunków i niepodleganiu wykluczeniu (załącznik nr 2 do niniejszego Zapytania Ofertowego),

   3) podpisana przez osobę reprezentującą oferenta klauzula informacyjna RODO (załącznik nr 3 do niniejszego zapytania ofertowego),

4) aktualny wypis z odpowiedniego rejestru (CEiDG, KRS),

5) umowę konsorcjum – w przypadku Wykonawców składających ofertę w konsorcjum,

6) pełnomocnictwo lub inny dokument potwierdzający umocowanie do reprezentowania Wykonawcy ubiegającego się o udzielenie zamówienia publicznego - pełnomocnictwo przekazuje się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. W przypadku, gdy pełnomocnictwo zostało wystawione w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu, opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej. Poświadczenia zgodności cyfrowego odwzorowania z pełnomocnictwem w postaci papierowej, może dokonać mocodawca (osoba/osoby wystawiające pełnomocnictwo) lub notariusz,

5. Brak powyższych informacji lub ich niezgodność z zasadą konkurencyjności lub brak poprawnego oznakowania załączników stanowić będzie o odrzuceniu oferty z powodów formalnych.
6. Oferta musi być podpisana przez osobę/y upoważnioną/e do reprezentowania Wykonawcy.
7. Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .xls .jpg (.jpeg) **ze szczególnym wskazaniem na .pdf.**
8. W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z formatów: .zip, .7Z.
9. Oferta, wnioski przedmiotowe i podmiotowe środki dowodowe, oświadczenia, wyjaśnienia, dokumenty składane elektronicznie muszą zostać podpisane elektronicznym kwalifikowanym podpisem lub podpisem zaufanym lub podpisem osobistym
10. Zamawiający zabrania modyfikacji treści dokumentów, za wyjątkiem miejsc służących do wypełnienia oferty.
11. Jakiekolwiek odstępstwo od wyżej opisanego sposobu przygotowania oferty jest równoznaczne z jej odrzuceniem, ze względu na niespełnienie kryteriów formalnych.
12. Zamawiający może w toku badania i oceny ofert żądać od Wykonawców wyjaśnień oraz dokumentów dotyczących treści złożonych ofert.
13. Wykonawca ponosi wszystkie koszty związane z przygotowaniem i złożeniem ofert.
14. Zamawiający nie zwraca Wykonawcom dokumentów zawartych w ofercie.

IX. MIEJSCE I TERMIN SKŁADANIA OFERT

1. Przygotowana zgodnie z powyższymi wytycznymi oferta wraz z wszystkimi wymaganymi przez Zamawiającego załącznikami i innymi dokumentami złożyć za pośrednictwem bazy konkurencyjności znajdującej się pod adresem: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/ nie później niż do dnia **05.09.2024r. do godziny 12:00**

2. W przypadku otrzymania przez Zamawiającego oferty po terminie podanym powyżej, oferta zostanie odrzucona.

X. INFORMACJE DOTYCZĄCE WYBORU NAJKORZYSTNIEJSZEJ OFERTY:

1. Oferty spełniające wymagania niniejszego zapytania ofertowego zostaną ocenione przez Zamawiającego zgodnie z przyjętymi kryteriami oceny.
2. W przypadku, gdy dla Zamawiającego oferta nie będzie zrozumiała może on się zwrócić do Wykonawcy o dodatkowe wyjaśnienia lub doprecyzowanie oferty.
3. Oferta zostanie odrzucona, jeśli:
   1) jej treść nie odpowiada treści niniejszego zapytania ofertowego,
   2) jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji,
   3) jest niezgodna z obowiązującymi przepisami prawa,
   4) jest niekompletna (np. brak załączników, brak podpisów na załącznikach, brak kompletnych danych w załącznikach).
   5) jeżeli będzie ona zawierała cenę brutto wyższą niż kwota, którą dysponuje Zamawiający na realizację przedmiotu zamówienia,
   6) gdy cena zaproponowana przez wykonawcę okaże się rażąco niska zgodnie z treścią rozdziału XVIII pkt.9 niniejszego zapytania ofertowego.
   7) Zawierająca błędy w obliczeniu ceny.

Z tytułu odrzucenia oferty Wykonawcy nie przysługuje żadne roszczenie przeciw Zamawiającemu.

XI. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca będzie związany ofertą przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. Wykonawca może przedłużyć termin związania ofertą, na czas niezbędny do zawarcia umowy, samodzielnie lub na wniosek Zamawiającego.

XII. OKREŚLENIE WARUNKÓW ISTOTNYCH ZMIAN UMOWY

Zamawiający przewiduje możliwość zmiany umowy.
Projekt umowy stanowi załącznik do niniejszego zapytania.

XIII. INFORMACJA O MOŻLIWOŚCI SKŁADANIAOFERT CZĘŚCIOWYCH

Zamawiający nie przewiduje możliwości składania ofert częściowych.

XIV. INFORMACJA O OFERTACH WARIANTOWYCH

Zamawiający nie dopuszcza składania ofert wariantowych.

XV. INFORMACJA O PLANOWANYCH ZAMÓWIENIACH UZUPEŁNIAJĄCYCH

Zamawiający nie planuje zamówień uzupełniających

XVI. INFORMACJA O PLANOWANYCH NEGOCJACJACH

Zamawiający nie planuje przeprowadzenia negocjacji

XVII. KONTAKT Z ZAMAWIAJĄCYM:

Osobami uprawnionymi do kontaktowania się z Wykonawcami i udzielania wyjaśnień dotyczących postępowania oraz w sprawach merytorycznych są:

1. Justyna Oferczak – Wydział Rozwoju tel. 042 288 81 73 email: europejski@powiat.zgierz.pl
2. Adrian Oszajca – Biuro Informatyki i Bezpieczeństwa Informacji tel. 042 288 81 41, email: adrian@powiat.zgierz.pl

XVIII. DODATKOWE POSTANOWIENIA:

1. Treść oferty musi odpowiadać treści niniejszego zapytania ofertowego.
2. Oferta powinna być sformułowana w języku polskim, przygotowana w sposób zrozumiały, czytelny i kompletny.
3. Oferent może przed upływem terminu składania ofert zmienić lub wycofać ofertę.
4. Oferent poda kwotę oferty w polskich złotych (PLN).
5. Wykonawca, z którym podpisana zostanie umowa będzie odpowiedzialni za przebieg oraz terminowe wykonanie zamówienia.
6. Wykonawca ponosi wszelkie koszty własne związane z przygotowaniem i złożeniem oferty, niezależnie od wyniku postępowania. Zamawiający nie odpowiada za koszty poniesione przez Wykonawcę w związku z przygotowaniem i złożeniem oferty.
7. Wykonawca proponując cenę oferty powinien wziąć pod uwagę wszelkie koszty, które mogą powstać w ramach realizacji zamówienia, szczególnie koszty związane z dojazdem do miejsca realizacji zamówienia. Zamawiający nie będzie refundował Wykonawcy zwiększonych kosztów wykonania zamówienia.
8. Wszelkie rozliczenia między Zamawiającym, a Wykonawcą dokonywane będą w złotych polskich (PLN).
9. Zamawiający może również odrzucić ofertę, gdy cena zaproponowana przez Wykonawcę okaże się rażąco niska, po uprzednim wezwaniu do złożenia wyjaśnień i nieuwzględnieniu tych wyjaśnień. Za cenę rażąco niską zostanie

uznana cena o 30% niższa od średniej arytmetycznej cen z wszystkich ofert złożonych w postępowaniu.

10. Zamawiający zastrzega sobie prawo do anulowania zapytania ofertowego bez podania przyczyny oraz unieważnienia postępowania w ramach zapytania ofertowego bez podania przyczyny – na każdym etapie – bez ponoszenia jakichkolwiek skutków prawnych finansowych.
11. Zamawiający zastrzega sobie prawo wydłużenia terminu składania ofert w ramach zapytania ofertowego bez podania przyczyny.

XIX. ZAŁĄCZNIKI

1. Formularz ofertowy – załącznik nr 1 do zapytania ofertowego.
2. Oświadczenie Wykonawcy o spełnieniu warunków i niepodleganiu wykluczeniu – załącznik nr 2 do zapytania ofertowego.
3. Informacja RODO – załącznik nr 3 do zapytania ofertowego.
4. Projekt wzoru Umowy – załącznik nr 4.

Signature Not Verified

Dokument podpisany przez Iwona Dąbek; Powiat Zgierski
Data: 2024.08.28 10:09:28 CEST

Signature Not Verified

Dokument podpisany przez Sebastian Dunin; Powiat Zgierski
Data: 2024.08.28 10:09:58 CEST