

Kunice dnia, 04.11.2024r.

**ZAPROSZENIE DO SKŁADANIA OFERT W POSTĘPOWANIU
O WARTOŚCI ZAMÓWIENIA NIEPRZEKRACZAJĄCEJ WYRAŻONEJ W ZŁOTYCH
RÓWNOWARTOŚCI KWOTY 130.000 złotych**

1. PEŁNA INFORMACJA O ZAMAWIAJĄCYM:

- Pełna nazwa zamawiającego: Gmina Kunice
- Adres: ulica Gwarna 1, 59-216 Kunice
- NIP: 691-21-46-015
- strona www: www.kunice.pl
- e-mail: kunice@kunice.pl
- telefon: (76) 8575322 wew. 10, fax: (76) 8575482
- kontakt telefoniczny w godzinach od 8:00 do 12:00 od poniedziałku do piątku

2. OPIS PRZEDMIOTU ZAMÓWIENIA:

Przedmiotem zamówienia jest **Dostawa sprzętu i oprogramowania informatycznego oraz usług w ramach programu Funduszy Europejskich na Rozwój Cyfrowy (FERC). Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23.** Umowa o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0744/ FERC.02.02-CS.01-001/23/2024

Dostawa: serwera RACK wraz z licencją na system Microsoft Windows 2022 (1 szt.), systemu serwerowego Microsoft Windows 2022 (1 szt.), zestawów kluczy U2F (12 szt.), zasilaczy awaryjnych UPS (20 szt.), oprogramowania antywirusowego dla stacji roboczych i serwerów (35 szt.), usługi serwisowej dla UTM Stormshield

Zamawiający dopuszcza składanie ofert częściowych tj. Wykonawcy mogą składać oferty na całość zamówienia lub na poszczególne części określone w tabelach formularza ofertowego.

Zamawiający zastrzega sobie prawo zakupu większej ilości wybranego asortymentu niż określona w ofercie Wykonawcy.

Opis przedmiotu zamówienia:

Część 1 zamówienia:

a) Serwer 1 szt. + 1 szt. System Windows Server 2022 (1 szt.) – kod cpv 48821000-9

Opis Parametru:	Wymagania minimalne:
Procesor	<ul style="list-style-type: none">• 1 procesor dedykowany do pracy z zaoferowanym serwerem o minimalnych wymaganiach:• ilość rdzeni: nie mniej niż 12, nie więcej niż 16• dostępnej pamięci cache nie mniejszej niż 16MB• taktowanie podstawowe min. 2,60 GHz z trybem pracy turbo;
Pamięć RAM	96 GB (DDR4 lub DDR5 RDIMM, Dual Rank, ECC)
Kontroler RAID	Sprzętowy, RAID 0/1/5/10 posiadający min. 1 GB pamięci flash

Obudowa	Na 4 dyski SSD, typ obudowy: RACK 1U
Dyski i napęd	4 x 960 GB SSD przeznaczone do pracy w serwerami
Karty sieciowe	<ul style="list-style-type: none"> 2 zintegrowane porty 1Gb Base-T (RJ-45) 2 x SFP+, 10 Gb/s
Zdalne zarządzanie	Moduł zdalnego zarządzania, diagnostyki i monitorowania pracy serwera z dedykowanym portem RJ-45
Ramka zabezpieczająca	Ramka zabezpieczająca chroniąca dyski twarde przed nieuprawnionym wyjęciem
Zasilanie	2x min. 600W (Hot-Plug, redundancja)
Systemy operacyjne	Microsoft Windows Server 2022 Standard (16 CORE)
Gwarancja	3 lata gwarancji Basic w trybie Next Business Day
Dodatkowe wymagania	<ul style="list-style-type: none"> Szyny montażowe – ruchome, 3 lata zachowania dysków twardych (KYHD) Serwer musi być fabrycznie nowy tj. nie może być wyprodukowany wcześniej niż rok przed datą dostawy oraz musi pochodzić z oficjalnego kanału dystrybucji na terenie Polski; Serwer w obudowie RACK

b) System Windows Server 2022 (1 szt.) – kod cpv 48620000-0

Opis Parametru:	Wymagania minimalne:
Nazwa	Microsoft Windows Server 2022 Standard (16 CORE)
Ilość	1 szt.

Część 2 zamówienia:

a) Klucze U2F – kod cpv 35120000-1 (6 zestawów po 2 klucze – 12 szt. kluczy)

Opis Parametru:	Wymagania minimalne:
Specyfikacja	Klucz bezpieczeństwa U2F (USB A)
Dodatkowe wymagania	<ul style="list-style-type: none"> Obsługa logowania do Windowsa przy pomocy specjalnej aplikacji. Możliwość przechowywanie kluczy GPG. Możliwość zabezpieczenia menadżera haseł KeePass/KeePassXC. Możliwość generowania i przechowywania haseł 2FA Możliwość logowania po SSH Obsługa NFC Adapter przejściówka z USB-C na USB-A do kluczy U2F (12 szt.)
Gwarancja	min. 12 miesięcy
Ilość	12 szt.

b) Zasilacze awaryjne UPS – 20 szt. – kod cpv 35100000-5

Opis Parametru:	Wymagania minimalne:
Moc	Pozorna min. 850VA

Gniazda wyjściowe	Schuko – min 3 szt
Gwarancja	min. 24 miesiące
Dodatkowe wymagania	<ul style="list-style-type: none"> • obudowa tower, • zabezpieczenia przeciwzwarciowe, przeciążeniowe i przeciwprzepięciowe, • wyświetlacz LCD
Architektura UPS	Line-Interactive
Ilość	20 szt.

Część 3 zamówienia:

a) Oprogramowanie antywirusowe – kod 48761000-0 (dla 35 użytkowników/serwerów)

Licencja na 18 miesięcy.

WYMAGANIA:

Administracja zdalna w chmurze:

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
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: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych:

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.

5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. 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).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez

wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera:

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, 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 możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.

4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
6. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszzonego mikro-serwisu.

Szyfrowanie:

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android:

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
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 skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: usunięcie zawartości urządzenia, przywrócenie urządzenia do ustawień fabrycznych, zablokowania urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS.

6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła.

Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość 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. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzewać jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: Czysty, Podejrzany, Bardzo podejrzany, Szkodliwy.
13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

b) Pakiet serwisowy do urządzenia UTM Stormshield – kod cpv 726110006

<i>Opis Parametru:</i>	<i>Wymagania minimalne:</i>
<i>Specyfikacja</i>	<i>Przedłużenie oraz rozszerzenie serwisu i licencji na 18 miesięcy dla UTM Stormshield (Premium UTM Security Pack na 18 miesięcy).</i>

Ewentualne podane w opisie lub pozostałej dokumentacji nazwy własne nie mają na celu naruszenia jakichkolwiek przepisów prawa, a mają jedynie sprecyzować oczekiwania jakościowe i techniczne Zamawiającego. Zamawiający dopuszcza rozwiązania równoważne pod warunkiem spełnienia tego samego poziomu technologicznego, technicznego, jakościowego i funkcjonalnego jako założony w projekcie. Wszystkie ewentualne nazwy własne i marki handlowe elementów, systemów, urządzeń i wyposażenia zawarte w dokumentacji mogą być zastąpione urządzeniami równoważnymi. Poprzez pojęcie urządzeń równoważnych należy rozumieć urządzenia gwarantujące realizację zamówienia

zgodnie z opisem przedmiotu zamówienia oraz zapewniające uzyskanie parametrów technicznych nie gorszych od założonych. Równoważne produkty i urządzenia muszą być dopuszczone do obrotu i stosowania zgodnie z obowiązującym prawem. Wykonawca, który zaproponuje produkty oraz urządzenia równoważne wymagające zmiany posiadanych decyzji, będzie musiał w ramach wykonania zamówienia w imieniu Zamawiającego, uzyskać wymagane decyzje własnym staraniem i kosztem, gwarantując jednocześnie wykonanie zamówienia w terminie wynikającym z zapytania ofertowego. Wykonawca, który powołuje się na rozwiązania równoważne z opisywanymi przez Zamawiającego, obowiązany jest wykazać, że oferowane przez niego dostawy spełniają wymagania postawione przez Zamawiającego. Obowiązek Wykonawcy wykazania równoważności produktu jest obowiązkiem wynikającym z ustawy, który może być spełniony w jakikolwiek sposób pozwalający Zamawiającemu jednoznacznie stwierdzić zgodność oferowanych w ofercie produktów z wymaganiami określonymi w opisie przedmiotu zamówienia, co powinno zostać wykazane na etapie składania ofert zawierających produkty równoważne.

3. Do obowiązków Wykonawcy należy:

- a) Dostawa przedmiotu zamówienia w części lub w całości (w zależności od złożonej oferty) do siedziby Zamawiającego tj. 59-216 Kunice ul. Gwarna 1 województwo dolnośląskie.
 - b) Dostawa przedmiotu zamówienia fabrycznie nowego, nieużywanego, wolnego od wad konstrukcyjnych, materiałowych i prawnych,
 - c) Dostarczony sprzęt musi zawierać komplet dokumentacji technicznej (koniecznie deklarację zgodności CE z odpowiednią dyrektywą, pod którą sprzęt podlega).
 - d) W przypadku oprogramowania, Wykonawca jest obowiązany do dostarczenia oświadczenia potwierdzającego, iż oferowana licencja systemu operacyjnego pochodzi z legalnego źródła i została zakupiona na terenie Rzeczypospolitej Polskiej.
4. Zamawiający dopuszcza możliwość zastosowania procedury sprawdzającej legalność oprogramowania poprzez zwrócenie się do przedstawiciela producenta oprogramowania z prośbą o weryfikację.
5. Wykonawca na dwa dni przed zaplanowaną dostawą poinformuje Zamawiającego o planowanym terminie dostawy do siedziby Zamawiającego.
6. Wykonawca w formularzu ofertowym, musi dokładnie wskazać model, kod producenta, który pozwoli określić zgodność oferowanego przedmiotu zamówienia z oczekiwaniami Zamawiającego.
7. Wykonawca do formularza ofertowego obowiązkowo załącza wypełniony załącznik nr 1 do formularza ofertowego, podając model i producenta oraz wypełniając wiersze określające zgodność oferowanego przedmiotu zamówienia z oczekiwaniami Zamawiającego.

8. Termin wykonania zamówienia i okres gwarancji

1. Maksymalny termin realizacji: do 30 dni od daty podpisania umowy. Minimalny okres gwarancji określa opis przedmiotu zamówienia opisany w treści zaproszenia do składania ofert – patrz tabele z poszczególnymi częściami zamówienia.

9. Udzielenie zamówienia mogą ubiegać się wykonawcy, którzy spełniają następujące warunki:

1. Zamawiający nie stawia wymagań.

10. Opis sposobu przygotowania oferty.

1. Oferty złożone po terminie nie będą rozpatrywane.
2. Oferent może przed upływem terminu składania ofert zmienić lub wycofać swoją ofertę.
3. W toku badania i oceny ofert Zamawiający może żądać od oferentów wyjaśnień dotyczących treści złożonych ofert, doświadczenia i kwalifikacji posiadanych przez Wykonawcę.
4. Oferta nie musi zostać podpisana kwalifikowanym podpisem elektronicznym, podpisem zaufanym ani podpisem osobistym. Dla ważności oferty wystarczające jest przesłanie skanu oferty z podpisem osoby/osób upoważnionej/ych. Natomiast umowa z wybranym wykonawcom musi zostać podpisana odręcznie lub poprzez kwalifikowany podpis elektroniczny, podpis zaufany lub osobisty.

5. Wraz z ofertą Wykonawca musi złożyć załącznik nr 1 do zapytania ofertowego.
6. Integralnym elementem zapytania ofertowego jest projekt umowy.

11. Opis sposobu obliczenia ceny oraz rodzaj i opis kryteriów, którymi będzie się kierował zamawiający przy wyborze oferty:

1. W postępowaniu jedynym kryterium jest najniższa cena.
2. Zamawiający informuje, że z postępowania wykluczy wszystkie podmioty lub osoby w stosunku do których zostanie wykazane, że istnieją przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. poz. 835).¹ na podstawie art. 5k rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 229 z 31.7.2014, str. 1), dalej: rozporządzenie 833/2014, w brzmieniu nadanym rozporządzeniem Rady (UE) 2022/576 w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 111 z 8.4.2022, str. 1).²

12. Miejsce, sposób i termin składania ofert:

1. Oferta powinna być przesłana elektronicznie poprzez platformę zakupową mieszczącą się pod adresem: <https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl> do dnia **12 listopada 2024r. do godziny 12:00**
2. W przypadku braku złożenia w wymaganym terminie formularza oferty Zamawiający uznaje samą ofertę za nieważną jednocześnie odrzucając ją z dalszego procesu porównania ofert. Natomiast w przypadku braku złożenia wraz z ofertą załącznika nr 1 do formularza oferty, Wykonawca zostanie wezwany do uzupełnienia w terminie 4 dni, po czym w przypadku braku przedłożenia dokumentów, oferta zostanie odrzucona.

Wójt Gminy Kunice
/-/ Krzysztof Błądziński

Załączniczki do zapytania ofertowego:

- 1. Formularz oferty*
- 2. Projekt umowy*

¹ Zgodnie z treścią art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:

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 ustawy;

2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 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 ustawy;

3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 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 ustawy.

² Zgodnie z treścią art. 5k ust. 1 rozporządzenia 833/2014 w brzmieniu nadanym rozporządzeniem 2022/576 zakazuje się udzielania lub dalszego wykonywania wszelkich zamówień publicznych lub koncesji objętych zakresem dyrektyw w sprawie zamówień publicznych, a także zakresem art. 10 ust. 1, 3, ust. 6 lit. a)–e), ust. 8, 9 i 10, art. 11, 12, 13 i 14 dyrektywy 2014/23/UE, art. 7 i 8, art. 10 lit. b)–f) i lit. h)–j) dyrektywy 2014/24/UE, art. 18, art. 21 lit. b)–e) i lit. g)–i), art. 29 i 30 dyrektywy 2014/25/UE oraz art. 13 lit. a)–d), lit. f)–h) i lit. j) dyrektywy 2009/81/WE na rzecz lub z udziałem:

- a) obywateli rosyjskich lub osób fizycznych lub prawnych, podmiotów lub organów z siedzibą w Rosji;
- b) osób prawnych, podmiotów lub organów, do których prawa własności bezpośrednio lub pośrednio w ponad 50 % należą do podmiotu, o którym mowa w lit. a) niniejszego ustępu; lub
- c) osób fizycznych lub prawnych, podmiotów lub organów działających w imieniu lub pod kierunkiem podmiotu, o którym mowa w lit. a) lub b) niniejszego ustępu,

w tym podwykonawców, dostawców lub podmiotów, na których zdolności polega się w rozumieniu dyrektyw w sprawie zamówień publicznych, w przypadku gdy przypada na nich ponad 10 % wartości zamówienia.

Informacja o przetwarzaniu danych osobowych

Zapytania ofertowe o wartości nie przekraczającej kwoty 30 000 euro – poza ustawą PZP

Zgodnie z art. 13 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) ,informujemy że:

- *Administratorem Pani/Pana danych osobowych jest: Wójt Gminy Kunice, ul. Gwarna 1, 59-216 Kunice, tel. 76/857-50-13, e-mail: kunice@kunice.pl*
- *W sprawach związanych z Pani/Pana danymi osobowymi proszę kontaktować się z Inspektorem Ochrony Danych (IOD): iodo@amt24.biz*
- *Pani/Pana dane osobowe będą przetwarzane w celu wyboru najkorzystniejszej oferty.*
- *Podstawą przetwarzania danych osobowych jest art. 6 pkt.1 lit. c RODO - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze zgodnie z ustawą z dnia 27 sierpnia 2009r. o finansach publicznych (Dz.U. 2009, poz. 1240) oraz art.6 pkt.1 lit. b RODO – przetwarzanie jest niezbędne do zawarcia i wykonania umowy.*
- *Odbiorca lub kategorie odbiorców: Podmioty upoważnione na podstawie zawartych umów powierzenia oraz uprawnione na mocy obowiązujących przepisów prawa.*
- *Pani/Pana dane osobowe będą przetwarzane przez okres niezbędny do realizacji celu przetwarzania, oraz przez okres wynikający z przepisów w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych, tj. 5 lat.*
- *Na każdym etapie przetwarzania danych osobowych przysługuje Pani/Panu prawo do:*
 - *sprostowania (poprawienia) danych,*
 - *ograniczenia przetwarzania danych,*
 - *dostępu do danych (w tym kopii tych danych)wniesienia skargi do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych Osobowych, /ul. Stawki 2, 00-193 Warszawa.*
- *W związku z przetwarzaniem danych na podstawie art. 6 ust. 1 lit. c RODO, nie przysługuje Pani/Panu prawo do:*
 - *wniesienia sprzeciwu wobec przetwarzania danych osobowych, na zasadach określonych w art. 21 RODO*
 - *usunięcia danych,*
 - *przenoszenia danych osobowych, o którym mowa w art. 20 RODO.*
- *Pani/Pana dane osobowe nie będą poddawane zautomatyzowanemu podejmowaniu decyzji, w tym również profilowaniu.*
- *Pani/Pana dane osobowe nie będą przekazywane do państw trzecich.*
- *Podanie danych jest wymogiem ustawowym.*
- *Konsekwencją niepodania danych osobowych będzie brak możliwości rozpatrzenia oferty.*