Cyberbezpieczne Wodociągi

ZAPYTANIE OFERTOWE WK.342.2.2026

na wykonanie zamówienia w zakresie

Zadanie 2 Obszar kompetencyjny: U28

Zadanie 3 Obszar techniczny IT

Zadanie 4 Obszar techniczny OT

w projekcie pn.

„Poprawa cyberbezpieczeństwa w Zakładzie Usług Gminnych Gmina Ełk Sp. z o.o.”

Zamawiający:

Zakład Usług Gminnych Gmina Ełk Sp. z o.o.

ul. Tadeusza Kościuszki 28A, 19-300 Ełk

NIP: 8481871071

Rozdział 1: ZAMAWIAJĄCY:

1. Nazwa i adres: **Zakład Usług Gminnych Gmina Ełk Sp. z o.o., ul. Tadeusza Kościuszki 28A, 19-300 Ełk, NIP: 8481871071,** województwo warmińsko-mazurskie.
2. Adres strony internetowej Zamawiającego: https://zug.elk.pl/
3. Postępowanie o udzielenie powyższego zamówienia prowadzone jest za pośrednictwem platformy zakupowej Baza Konkurencyjności dostępnej pod adresem https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/

Rozdział 2: TRYB UDZIELENIA ZAMÓWIENIA:

1. Zamawiający informuje, że jest zamawiającym publicznym sektorowym, w rozumieniu art. 4 pkt 3 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2024r. poz. 1320 z poźn. zm. – w dalszej części „ustawa Pzp" lub „Pzp"), który wykonuje działalność sektorową w zakresie gospodarki wodnej (art. 5 ust. 4 pkt. 1 ustawy Pzp).
2. Szacowana wartość zamówienia nie przekracza kwoty 432 000 euro, co stanowi równowartość kwoty 1 861 920 zł.
3. W związku z powyższym do czynności podejmowanych przez Zamawiającego i Wykonawców w postępowaniu o udzielenie zamówienia publicznego nie stosuje się przepisów ustawy z dnia 11 września 2019 r. Prawo Zamówień Publicznych (Dz.U. z 2026 r., poz. 793 t.j. – dalej jako „pzp").
4. Postępowanie o udzielenie powyższego zamówienia prowadzone jest na zasadach określonych Regulaminem udzielania zamówień w projektach współfinansowanych lub finansowanych ze środków zewnętrznych w przez Zakładzie Usług Gminnych Gmina Ełk Sp. z o.o.
5. Do postępowania ma zastosowanie Regulamin Konkursu Grantowego pn. "Cyberbezpieczne Wodociągi" Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo: "Cyberbezpieczeństwo – Cyberbezpieczne Wodociągi". Krajowy Plan Odbudowy i Zwiększania Odporności finansowany ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności.
6. Oznaczenie postępowania: postępowanie posiada znak spraw **WK.342.2.2026** Zaleca się, aby Wykonawcy we wszelkich kontaktach z Zamawiającym powoływali się na wyżej wskazane oznaczenie.
7. Postępowanie prowadzone jest w oparciu o wytyczne Reguły Konkurencyjności.
8. W zakresie nieuregulowanym OPZ zastosowanie mają przepisy ustawy Kodeks cywilny. Postępowanie prowadzone jest w języku polskim.

Rozdział 3: NAZWA, PRZEDMIOT ZAMÓWIENIA:

1. Przedmiotem niniejszego zamówienia jest: Dostawa i wdrożenie sprzętu, usług i oprogramowania oraz przeprowadzenie szkoleń technicznych w ramach projektu pn. „Poprawa cyberbezpieczeństwa w Zakładzie Usług Gminnych Gmina Ełk Sp. z o.o." realizowanego w ramach Inwestycji C3.1.1 „Cyberbezpieczeństwo – CyberPL" – Cyberbezpieczne Wodociągi, finansowanego z Krajowego Planu Odbudowy i Zwiększania Odporności.
2. Zamawiający nie dokonał podziału zamówienia na części. Obszary techniczny IT oraz techniczny OT muszą stanowić nierozerwalną całość realizowaną przez jednego Wykonawcę, co jest warunkiem koniecznym dla zachowania pełnej spójności wdrożeniowej zintegrowanego ekosystemu bezpieczeństwa oraz zapewnienia zgodności z wymogami ustawy o Krajowym Systemie Cyberbezpieczeństwa. Integralność ta jest również niezbędna do przeprowadzenia specjalistycznych szkoleń stanowiskowych, które jako kluczowy element procesu wdrożenia muszą być ściśle dostosowane do unikalnej konfiguracji dostarczonego sprzętu i oprogramowania, zapewniając personelowi kompetencje niezbędne do poprawnej interpretacji alertów oraz efektywnego zarządzania nowym systemem w specyficznym środowisku Zamawiającego.
3. Zamawiający nie dopuszcza możliwości składania ofert częściowych. Wykonawca może złożyć ofertę na jedną ofertę.
4. Szczegółowy opis przedmiotu zamówienia przedstawiony jest w Załączniku nr 2 do zapytania ofertowego – Opis Przedmiotu Zamówienia (OPZ)
5. Wykonawca zobowiązany jest do oznakowania dostarczonego sprzętu oraz dokumentacji projektowej logotypami (KPO, barwy narodowe, UE NextGenerationEU) zgodnie z Księgą Identyfikacji Wizualnej KPO.
6. Realizacja zadania musi być zgodna z zasadą DNSH (Do No Significant Harm – nie czyń znaczącej szkody). Zastosowane rozwiązania powinny być zgodne celami środowiskowymi zasady DNSH. Szczegółowe wytyczne w tym zakresie zawierają następujące dokumenty:

− Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2020/852 z dnia 18 czerwca 2020 r. w sprawie ustanowienia ram ułatwiających zrównoważone inwestycje, zmieniające rozporządzenie (UE) 2019/2088
− Rozporządzenie delegowane Komisji (UE) 2021/2139 z dnia 4 czerwca 2021 r.
− Rozporządzenie delegowane Komisji (UE) 2023/2486 z dnia 27 czerwca 2023 r.
− Źródła informacji dotyczące zasady DNSH - https://www.kpo.gov.pl/strony/okpo/dla-instytucji/dokumenty/dnsh/

7. Jeżeli gdziekolwiek w OPZ przedmiot zamówienia określony został przez wskazanie znaków towarowych, patentów lub pochodzenia to Zamawiający dopuszcza w tym zakresie składanie ofert przy zastosowaniu rozwiązań równoważnych opisywanym. Tam, gdzie w opisie przedmiotu zamówienia zostało wskazane pochodzenie urządzeń objętych zamówieniem (np. marka, znak towarowy, producent, dostawca), Zamawiający dopuszcza oferowanie urządzeń o parametrach równoważnych - tożsamych lub wyższych od tych, jakie zawarto w opisie. Pod pojęciem równoważności rozumieć należy, iż zagwarantują one realizację zamówienia w zgodzie z opisem przedmiotu zamówienia oraz zapewnią uzyskanie parametrów techniczno-jakościowych oraz wymogów gwarancyjnych, nie gorszych od

założonych w w/w opisie. Podane w opisach przedmiotu zamówienia nazwy własne, mają jedynie za zadanie sprecyzowanie oczekiwań jakościowych, technicznych i technologicznych Zamawiającego. Opis kryteriów równoważności wynika z wymaganych parametrów (odpowiednio dla poszczególnych elementów dostawy), wg Opisu Przedmiotu Zamówienia, stanowiącego załącznik nr 2 do zapytania ofertowego.

8. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać w treści oferty, że oferowane przez niego dostawy i usługi spełniają wymagania określone przez Zamawiającego. Ciężar udowodnienia równoważności spoczywa na Wykonawcy, co oznacza, że wraz z ofertą winien on złożyć dokumenty (np. karty katalogowe, certyfikaty, specyfikacje techniczne, zdjęcia), z których w sposób jednoznaczny i niebudzący wątpliwości wynikać będzie, że oferowane rozwiązania posiadają parametry nie gorsze niż te wskazane w Opisie Przedmiotu Zamówienia.
9. Opis Przedmiotu Zamówienia według kodów Wspólnego Słownika Zamówień (CPV).

30200000-1	Urządzenia komputerowe
32420000-3	Urządzenia sieciowe
32422000-7	Elementy składowe sieci
35100000-5	Urządzenia awaryjne i zabezpieczające
35121000-8	Urządzenia ochronne
48000000-8	Pakiety oprogramowania i systemy informatyczne
48210000-3	Pakiety oprogramowania dla sieci
48600000-4	Pakiety oprogramowania dla baz danych i operacyjne
48730000-4	Pakiety oprogramowania zabezpieczającego
48732000-8	Pakiety oprogramowania do zabezpieczania danych
48820000-2	Serwery
48821000-9	Serwery sieciowe
48900000-7	Różne pakiety oprogramowania i systemy komputerowe
51611100-9	Usługi instalowania urządzeń komputerowych
72222000-7	Usługi w zakresie systemów informacji lub strategicznej analizy technologicznej oraz usługi w zakresie planowania
72263000-6	Usługi wdrażania oprogramowania
72265000-0	Usługi konfiguracji oprogramowania
72315000-6	Usługi zarządzania siecią danych oraz usługi wspierające
72600000-6	Usługi doradcze i dodatkowe w zakresie sprzętu komputerowego
73431000-2	Testowanie i ocena systemów bezpieczeństwa
79417000-0	Usługi doradcze w zakresie bezpieczeństwa
80510000-2	Usługi szkolenia specjalistycznego
80533100-0	Usługi szkolenia komputerowego
80550000-4	Usługi szkolenia w dziedzinie bezpieczeństwa

10. Wykonawca ponosi wyłączną odpowiedzialność za wszelkie szkody będące następstwem niewykonania lub nienależytego wykonania przedmiotu umowy, które to szkody Wykonawca zobowiązuje się pokryć w pełnej wysokości.
11. Cena oferty jest ceną ryczałtową i obejmuje wszystkie koszty konieczne do wykonania zamówienia.

Rozdział 4: TERMIN WYKONANIA ZAMÓWIENIA

1. Wykonawca jest zobowiązany wykonać przedmiot zamówienia w terminie do **30 dni** od dnia podpisania umowy, maksymalnie do **28 grudnia 2026 r.**
2. Zamawiający przewiduje możliwość wydłużenia terminu realizacji umowy na zasadach opisanych w projektowanych postanowieniach umowy, o ile zmiana ta nie spowoduje przekroczenia końcowej daty kwalifikowalności wydatków w projekcie.
3. Zamawiający wyjaśnia, że powyższy termin dotyczy wykonania dostaw, wdrożeń i pozostałych czynności niezbędnych do dokonania odbioru końcowego. Usługi gwarancyjne, utrzymania oraz wsparcia technicznego będą realizowane w okresach określonych w dokumentacji postępowania.

Rozdział 5: INFORMACJE UZUPEŁNIAJACE

1. Zamawiający wymaga od Wykonawcy przeprowadzenia wizji lokalnej i zapoznanie się ze stanem faktycznym i dokumentacją infrastruktury Zamawiającego w celu złożenia oferty.
2. **Wizja lokalna i sprawdzenie dokumentów**

a) Ze względu na specyfikę przedmiotu zamówienia, obejmującego systemy/infrastrukturę teleinformatyczną/usługi z zakresu cyberbezpieczeństwa], której pełne odwzorowanie w opisie przedmiotu zamówienia nie jest możliwe, Zamawiający **wymaga** złożenia oferty po odbyciu przez Wykonawcę wizji lokalnej oraz po sprawdzeniu dokumentów infrastruktury Zamawiającego dostępnych na miejscu.

b) Wizja lokalna ma charakter **obowiązkowy**. Odbycie wizji lokalnej i sprawdzenie udostępnionych dokumentów nie stanowi warunku udziału w postępowaniu, lecz jest czynnością, której zaniechanie skutkuje odrzuceniem oferty.

c) W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia (konsorcjum) wymóg, o którym mowa w ust. 1, uznaje się za spełniony, jeżeli wizję lokalną odbędzie co najmniej jeden z wykonawców lub należycie umocowany przedstawiciel działający w imieniu wszystkich wykonawców wspólnie ubiegających się o zamówienie. Zamawiający nie wymaga odrębnego udziału każdego z członków konsorcjum.

d) Warunkiem dopuszczenia do udziału w wizji lokalnej jest:

1. **zgłoszenie** udziału na adres **sekretariat@zug.elk.pl** w terminie ze wskazaniem imienia, nazwiska i numeru dokumentu tożsamości każdej z osób osoby ze strony danego wykonawcy);
2. **podpisanie zobowiązania do zachowania poufności (NDA)**, przed udostępnieniem jakichkolwiek dokumentów i informacji o infrastrukturze. A po zakończeniu postępowania do trwałego usunięcia danych Zamawiającego poprzez nadpisywanie nośników w co najmniej 5 cyklach (Level 5), zgodnie z uznaną metodą sanityzacji

danych (np. HMG Infosec Standard 5, NIST SP 800-88) lub metodą równoważną, z weryfikacją skuteczności nadpisania i potwierdzeniem wykonania w formie raportu z kasowania.

e) W trakcie wizji lokalnej obowiązuje **zakaz utrwalania** (fotografowania, nagrywania, kopiowania) dokumentacji, konfiguracji oraz elementów infrastruktury, chyba że Zamawiający wyrazi na to pisemną zgodę. Dokumenty zawierające informacje wrażliwe (m.in. topologia sieci, schematy zabezpieczeń, konfiguracje, dane o podatnościach) udostępniane są wyłącznie do wglądu na miejscu, w wydzielonym pomieszczeniu, pod nadzorem przedstawiciela Zamawiającego.

f) Zamawiający zapewnia wszystkim wykonawcom **jednakowe warunki** odbycia wizji lokalnej. W razie zgłoszenia się większej liczby Wykonawców, Zamawiający może wyznaczyć dodatkowe terminy, zapewniając równe traktowanie. Odbycie wizji lokalnej nie pozbawia Wykonawcy prawa do zwrócenia się o wyjaśnienie treści OPZ.

g) Koszty udziału w wizji lokalnej ponosi we własnym zakresie Wykonawca.

3. Zamawiający nie dopuszcza złożenia ofert wariantowych.
4. Zamawiający nie przewiduje zawarcia umowy ramowej.
5. Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej.
6. Zamawiający nie zamierza ustanowić dynamicznego systemu zakupów.
7. Zamawiający nie przewiduje rozliczenia w walutach obcych.
8. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
9. Zamawiający nie przewiduje udzielenia zaliczek na poczet wykonania zamówienia.

Rozdział 6: INFORMACJE O ŚRODKACH KOMUNIKACJI ELEKTRONICZNEJ, PRZY UŻYCIU KTÓRYCH ZAMAWIAJĄCY BĘDZIE KOMUNIKOWAŁ SIĘ Z WYKONAWCAMI ORAZ INFORMACJE O WYMAGANIACH TECHNICZNYCH I ORGANIZACYJNYCH SPORZĄDZANIA, WYSYŁANIA I ODBIERANIA KORESPONDENCJI ELEKTRONICZNEJ:

1. W postępowaniu o udzielenie zamówienia komunikacja, między Zamawiającym a Wykonawcami, w tym składanie ofert oraz pytań o wyjaśnienie treści zapytania ofertowego, odbywa się drogą elektroniczną wyłącznie za pośrednictwem Bazy Konkurencyjności (BK2021), dostępnej pod adresem: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/
2. Wymagania techniczne i organizacyjne korzystania z Bazy Konkurencyjności:
   a. Rejestracja oraz udział w postępowaniach za pośrednictwem Bazy Konkurencyjności są bezpłatne.
   b. Szczegółowe instrukcje dotyczące obsługi systemu, w tym wymagania techniczne dla sprzętu i oprogramowania Wykonawcy, znajdują się w sekcji «Pomoc» pod adresem: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/pomoc.

c. Pomoc techniczna jest dostępna zgodnie z informacjami zamieszczonymi w sekcji «Pomoc» Bazy Konkurencyjności

3. Oświadczenia, wnioski oraz dokumenty przekazywane są w formacie elektronicznym. Oferta wraz z załącznikami musi zostać sporządzona w postaci elektronicznej i opatrzona kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. Zamawiający rekomenduje format plików .pdf.
4. Wykonawca składa wniosek o wyjaśnienie treści zapytania ofertowego wraz z załącznikami wyłącznie za pośrednictwem funkcjonalności Bazy Konkurencyjności. Zamawiający udzieli wyjaśnień niezwłocznie, pod warunkiem, że wniosek wpłynął do Zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert (zgodnie z procedurą wyboru wykonawców).
5. W przypadku, gdy wniosek o wyjaśnienie treści zapytania ofertowego wraz z załącznikami nie wpłynie w terminie, Zamawiający nie ma obowiązku udzielania wyjaśnień zapytania ofertowego wraz z załącznikami oraz przedłużenia terminu składania ofert. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści zapytania ofertowego wraz z załącznikami.
6. Zamawiający udzieli odpowiedzi na wszelkie zapytania niezwłocznie, jeżeli prośba o wyjaśnienie treści zapytania ofertowego wraz z załącznikami wpłynęła w terminie zgodnym z pkt. 4.
7. Zamawiający opublikuje odpowiedzi i modyfikacje na stronie prowadzonego postępowania bez ujawniania źródła zapytania.
8. We wszelkiej korespondencji dotyczącej niniejszego postępowania Zamawiający oraz Wykonawcy posługują się oznaczeniem sygnatury sprawy (nadanym przez Zamawiającego) **WK.342.2.2026** Po upływie terminu składania ofert korespondencja dotycząca badania i oceny ofert, w szczególności wezwania do wyjaśnień lub uzupełnień oraz odpowiedzi na te wezwania, odbywa się za pośrednictwem poczty elektronicznej. Adres Zamawiającego do tej korespondencji: **sekretariat@zug.elk.pl** . Zamawiający kieruje korespondencję na adres Wykonawcy wskazany w ofercie. Na żądanie drugiej strony należy niezwłocznie potwierdzić otrzymanie korespondencji. Powyższe nie dopuszcza składania ofert pocztą elektroniczną.

Rozdział 7: WARUNKI UDZIAŁU W POSTĘPOWANIU, PODSTAWY WYKLUCZENIA WYKONAWCY ORAZ PRZESŁANKI ODRZUCENIA OFERTY

7.1. Warunki udziału w postępowaniu

1. Wykonawca na dzień składania ofert musi spełniać warunki udziału w postępowaniu dotyczące:

   a) kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów.

   Zamawiający nie stawia szczególnych wymagań w tym zakresie.

   b) sytuacji ekonomicznej lub finansowej.

   Wykonawca w okresie realizacji przedmiotu zamówienia musi posiadać aktualne ubezpieczenie od odpowiedzialności cywilnej w zakresie ryzyk cybernetycznych prowadzonej działalności na sumę gwarancyjną nie mniejszą niż 300 000,00 zł. Wykonawca

utrzyma ważność ubezpieczenia przez cały okres realizacji Umowy oraz cały okres gwarancji, utrzymania i wsparcia. Zamawiający nie wymaga, aby jedna polisa obejmowała cały wieloletni okres gwarancji i wsparcia. Dopuszczalne jest utrzymywanie ciągłości ochrony poprzez odnawianie polis na kolejne okresy ubezpieczenia. Warunkiem jest zachowanie nieprzerwanej ochrony ubezpieczeniowej oraz wymaganej sumy gwarancyjnej nie niższej niż 300 000,00 zł przez cały okres wskazany w dokumentacji zamówienia.

c) zdolności technicznej lub zawodowej.

I. Wykonawca spełni warunek, jeżeli wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, należycie wykonał co najmniej 2 zamówienia o złożonym charakterze dotyczące infrastruktury teleinformatycznej lub cyberbezpieczeństwa. Każde z wykazanych zamówień musi obejmować co najmniej 5 z następujących obszarów:

1. NGFW/UTM;
2. switching/routing/VLAN;
3. WLAN/NAC/802.1X;
4. serwery/wirtualizacja;
5. storage/NAS;
6. backup/DR;
7. AD/IAM;
8. MFA/PKI;
9. SIEM;
10. hardening;
11. endpoint management;
12. testy bezpieczeństwa.

II. Wykonawca spełni warunek, jeżeli wykaże łącznie w ramach przedstawionego doświadczenia:

1) co najmniej jedno wdrożenie SIEM obejmujące monitorowanie systemów, endpointów lub agentów;
2) co najmniej jedno wdrożenie obejmujące NGFW, segmentację VLAN oraz integrację z co najmniej jednym z następujących rozwiązań: AD, LDAP, RADIUS lub MFA;
3) co najmniej jedno wdrożenie backup/DR obejmujące rzeczywiste i udokumentowane odtworzenie danych lub systemu;
4) co najmniej 2 audyty cyberbezpieczeństwa, z których każdy obejmował co najmniej 4 z następujących obszarów:

a. SZBI lub audyt organizacyjny,
b. zarządzanie ryzykiem,
c. infrastruktura sieciowa,
d. Active Directory,
e. vulnerability assessment lub testy penetracyjne,
f. NGFW,
g. backup/DR,
h. aplikacje,
i. socjotechnika.

Jedna realizacja może potwierdzać spełnienie więcej niż jednego wymagania, jeżeli jej rzeczywisty zakres obejmował wszystkie wykazywane elementy. Udokumentowane odtworzenie danych lub systemu w obszarze backup/DR oznacza przeprowadzenie rzeczywistego albo kontrolowanego testu odtworzenia. Jego wykonanie może zostać potwierdzone protokołem testu, protokołem odbioru lub innym dokumentem pochodzącym od odbiorcy usługi, jednoznacznie potwierdzającym zakres oraz wynik przeprowadzonych czynności.

Zamawiający nie wymaga określonej formy dokumentu, o ile przedstawione informacje pozwalają na obiektywną ocenę spełnienia warunku.

III. Wykonawca wykaże, że dysponuje lub będzie dysponował zespołem osób posiadających kwalifikacje, wiedzę i doświadczenie niezbędne do należytej realizacji przedmiotu zamówienia. Zespół skierowany do realizacji zamówienia musi obejmować co najmniej 7 różnych osób. Jedna osoba może pełnić nie więcej niż 3 funkcje określone w niniejszych wymaganiach, pod warunkiem że spełnia wszystkie wymagania przewidziane dla każdej z powierzonych jej funkcji. Samo posiadanie certyfikatu lub zaświadczenia albo ukończenie szkolenia nie jest wystarczające, jeżeli dla danej funkcji wymagane jest również doświadczenie praktyczne. Ten sam projekt może służyć do wykazania doświadczenia jednej osoby dla kilku funkcji wyłącznie wtedy, gdy Wykonawca wskaże, jakie czynności osoba ta wykonywała osobiście w zakresie każdej z tych funkcji. Osoby wskazane w celu potwierdzenia spełnienia warunków muszą faktycznie uczestniczyć w realizacji zamówienia. W przypadku zmiany osoby w trakcie realizacji zamówienia Wykonawca zapewni zastępstwo przez osobę spełniającą wszystkie wymagania określone dla danej funkcji na poziomie nie niższym niż osoba zastępowana.

1) Kierownik Techniczny / Architekt Cyberbezpieczeństw - Wykonawca zapewni co najmniej jedną osobę, która:

I. posiada co najmniej 7 lat doświadczenia zawodowego w IT, w tym co najmniej 5 lat doświadczenia w cyberbezpieczeństwie, projektowaniu infrastruktury lub architekturze systemów teleinformatycznych;
II. uczestniczyła w co najmniej 3 zakończonych projektach obejmujących budowę, modernizację, migrację lub zabezpieczenie infrastruktury teleinformatycznej;
III. uczestniczyła w co najmniej 2 projektach obejmujących integrację co najmniej 3 z następujących obszarów:
    a. LAN/WAN/WLAN,
    b. NGFW/UTM,
    c. Active Directory/IAM,
    d. MFA/PKI,
    e. SIEM,
    f. wirtualizacja,
    g. backup/DR,
    h. storage/NAS,
    i. endpoint security,
    j. hardening;
IV. w co najmniej 2 projektach pełniła funkcję kierownika technicznego, architekta, głównego inżyniera lub osoby odpowiedzialnej za integrację techniczną;
V. posiada doświadczenie w przygotowaniu, zatwierdzaniu lub odbiorze co najmniej 3 z następujących rodzajów dokumentacji:
    a. HLD,
    b. LLD,
    c. plan wdrożenia,
    d. plan migracji,
    e. plan rollback,
    f. plan testów,
    g. dokumentacja powdrożeniowa,

h. plan backupu/DR;

VI. posiada co najmniej jeden certyfikat potwierdzający kompetencje w zakresie cyberbezpieczeństwa, inżynierii bezpieczeństwa lub zarządzania bezpieczeństwem na poziomie co najmniej średniozaawansowanym, np. CySA+, CASP+, CISSP, CISM lub równoważny;

2) Ekspert ds. Ciągłości Działania / BCM / DR - Wykonawca zapewni co najmniej jedną osobę, która:

I. posiada co najmniej 3 lata doświadczenia w zakresie ciągłości działania, Disaster Recovery, bezpieczeństwa informacji lub zarządzania ryzykiem;

II. uczestniczyła w co najmniej 2 projektach, z których każdy obejmował co najmniej 2 z następujących obszarów:

a. BIA,

b. BCP,

c. DRP,

d. RTO/RPO,

e. procedury awaryjne,

f. procedury odtworzeniowe;

III. uczestniczyła w co najmniej jednym rzeczywistym lub kontrolowanym teście ciągłości działania albo odtworzenia;

IV. posiada certyfikat lub ukończyła specjalistyczne szkolenie dotyczące ISO 22301 albo rozwiązania równoważnego;

V. posiada doświadczenie lub wiedzę pozwalającą uwzględnić zależności IT–OT w BIA, BCP i DRP.

3) Senior Inżynier Sieci i Bezpieczeństwa Sieciowego / NGFW - Wykonawca zapewni co najmniej jedną osobę, która:

I. posiada co najmniej 5 lat doświadczenia w sieciach komputerowych, w tym co najmniej 3 lata doświadczenia w bezpieczeństwie sieciowym;

II. uczestniczyła w co najmniej 3 produkcyjnych wdrożeniach infrastruktury sieciowej;

III. uczestniczyła w co najmniej 2 wdrożeniach obejmujących switching, routing lub VLAN;

IV. uczestniczyła w co najmniej 2 wdrożeniach rozwiązań klasy NGFW/UTM;

V. posiada doświadczenie w zakresie:

a. VLAN,

b. trunking,

c. STP/RSTP/MSTP,

d. routingu,

e. ACL,

f. zabezpieczeń warstwy L2,

g. 802.1X,

h. RADIUS,

i. VPN,

j. polityk firewall;

VI. posiada co najmniej jedną techniczną kwalifikację z zakresu sieci komputerowych;

VII. posiada certyfikat techniczny lub ukończyła autoryzowane szkolenie dotyczące faktycznie zaoferowanego produktu NGFW lub jego rodziny produktowej;

VIII. uczestniczyła w co najmniej jednym wdrożeniu NGFW dotyczącym faktycznie zaoferowanego produktu lub jego rodziny produktowej;

IX. wdrożenie, o którym mowa w pkt 8, zostało zakończone w okresie ostatnich 5 lat przed upływem terminu składania ofert;

X. uczestniczyła w co najmniej jednym wdrożeniu obejmującym co najmniej 4 z następujących elementów:

a. firewall policies,

b. NAT,

c. VPN,

d. IPS/Threat Prevention,

e. URL Filtering,

f. Application Control,
g. LDAP/AD,
h. RADIUS/MFA,
i. centralne zarządzanie,
j. integrację z SIEM.6. Inżynier SIEM / Wazuh / Linux

4) Specjalista Linux - Wykonawca zapewni co najmniej jedną osobę, która:

I. posiada co najmniej 4 lata doświadczenia w pracy z systemami Linux, systemami bezpieczeństwa lub rozwiązaniami centralnego logowania;
II. posiada co najmniej 2 lata doświadczenia w pracy z systemami SIEM;
III. uczestniczyła w co najmniej 2 produkcyjnych wdrożeniach lub istotnych modernizacjach systemów SIEM;
IV. wykonywała co najmniej 5 z następujących czynności:
a. instalacja agentów,
b. integracja źródeł logów,
c. konfiguracja kolektorów,
d. konfiguracja reguł,
e. konfiguracja alertów,
f. konfiguracja paneli i dashboardów,
g. FIM,
h. vulnerability detection,
i. SCA/CIS,
j. Active Response,
k. tuning false positives;
V. posiada doświadczenie w co najmniej jednym środowisku obejmującym jednocześnie systemy Windows i Linux;
VI. posiada formalne techniczne potwierdzenie kompetencji dotyczących faktycznie zaoferowanego systemu SIEM;
VII. uczestniczyła w co najmniej jednym wdrożeniu dotyczącym zaoferowanego produktu lub jego rodziny;

VIII. wdrożenie, o którym mowa w pkt 7, zostało zakończone w okresie ostatnich 5 lat przed upływem terminu składania ofert.

5) Specjalista ds. Walidacji Zabezpieczeń i Zarządzania Podatnościami - Wykonawca zapewni co najmniej jedną osobę, która:
   I. posiada co najmniej 4 lata doświadczenia w cyberbezpieczeństwie;
   II. uczestniczyła w co najmniej 2 projektach obejmujących vulnerability management, SOC, SIEM, incident response, threat detection, hardening lub security validation;
   III. posiada doświadczenie w:
      a. analizie wyników skanowania podatności,
      b. analizie CVE,
      c. klasyfikacji i priorytetyzacji ryzyka,
      d. identyfikowaniu false positives,
      e. walidacji wdrożonych poprawek,
      f. weryfikacji detekcji SIEM;
   IV. posiada co najmniej jeden certyfikat na poziomie średniozaawansowanym lub zaawansowanym, np. CASP+, CySA+, BTL2, GCIH, GCIA, ECIH lub równoważny.
   V. Do zakresu tej funkcji należy w szczególności:
      a. walidacja podatności;
      b. weryfikacja skuteczności hardeningu;
      c. korelacja wyników testów bezpieczeństwa z danymi i zdarzeniami rejestrowanymi przez SIEM;
      d. wsparcie klasyfikacji CVE/CVSS;
      e. walidacja działań naprawczych;
      f. wsparcie retestów.

6) Specjalista ds. Technicznych Testów Bezpieczeństwa / Penetration Tester - Wykonawca zapewni co najmniej jedną osobę, która:
   I. posiada co najmniej 4 lata doświadczenia w technicznych testach bezpieczeństwa, audytach technicznych lub testach penetracyjnych;

II. uczestniczyła w co najmniej 4 zakończonych testach bezpieczeństwa lub testach penetracyjnych;

III. posiada doświadczenie obejmujące łącznie:

a. Active Directory lub inny system tożsamości,

b. infrastrukturę sieciową,

c. publicznie dostępne usługi internetowe,

d. aplikację lub system aplikacyjny;

IV. posiada co najmniej jeden praktyczny certyfikat techniczny, np.:

a. OSCP,

b. OSEP,

c. OSWE,

d. PNPT,

e. CRTO,

f. eCPPT,

g. eWPTX,

h. lub równoważny.

V. Certyfikat oparty wyłącznie na egzaminie teoretycznym nie jest samodzielnie równoważny certyfikatowi praktycznemu.

7) Inżynier Wirtualizacji, Backupu, Storage i NAS - Wykonawca zapewni co najmniej jedną osobę, która:

I. posiada co najmniej 5 lat doświadczenia w zakresie infrastruktury serwerowej, wirtualizacji, backupu lub pamięci masowej;

II. uczestniczyła w co najmniej 3 projektach infrastrukturalnych;

III. uczestniczyła w co najmniej jednym projekcie obejmującym łącznie:

a. co najmniej 2 hosty wirtualizacyjne,

b. storage lub repozytorium,

c. backup maszyn wirtualnych,

d. testowe odtworzenie;

IV. uczestniczyła w co najmniej jednym projekcie obejmującym klaster, HA lub inne rozwiązanie zapewniające redundancję;

V. posiada doświadczenie w co najmniej 2 wdrożeniach środowisk wirtualizacyjnych, w tym w co najmniej jednym wdrożeniu dotyczącym zaoferowanej platformy lub jej rodziny;

VI. posiada doświadczenie w co najmniej 2 wdrożeniach systemów backupowych, w tym w co najmniej jednym wdrożeniu dotyczącym zaoferowanego systemu lub jego rodziny;

VII. posiada doświadczenie w co najmniej 2 wdrożeniach storage/NAS obejmujących RAID, wolumeny, LUN lub udziały sieciowe oraz integrację z systemem backupu lub wirtualizacji;

VIII. posiada co najmniej jedno wymagane doświadczenie produktowe dotyczące kluczowej zaoferowanej platformy, pochodzące z projektu zakończonego w okresie ostatnich 5 lat przed upływem terminu składania ofert;

IX. posiada techniczny certyfikat lub ukończyła techniczne szkolenie dotyczące zaoferowanego rozwiązania, jeżeli dla danej platformy funkcjonuje odpowiedni program certyfikacji lub szkoleń technicznych.

8) Inżynier Microsoft / AD / IAM / PKI / MFA / Endpoint - Wykonawca zapewni co najmniej jedną osobę, która:

I. posiada co najmniej 5 lat doświadczenia w pracy z Windows Server i Active Directory;

II. uczestniczyła w co najmniej 2 produkcyjnych wdrożeniach lub istotnych modernizacjach Active Directory;

III. posiada doświadczenie w co najmniej 5 z następujących obszarów:

a. AD DS,
b. GPO,
c. DNS,
d. DHCP,
e. LAPS,
f. BitLocker,
g. WSUS,

h. Defender,
i. Credential Guard,
j. WDAC/AppLocker,
k. AD CS/PKI,
l. NPS/RADIUS,
m. PAW;

IV. posiada formalne potwierdzenie kompetencji w zakresie Windows Server, Active Directory, GPO, PKI lub bezpieczeństwa rozwiązań Microsoft.

9) Specjalista MFA - Osoba odpowiedzialna za MFA musi dodatkowo:
   I. posiadać formalne techniczne potwierdzenie kompetencji dotyczących zaoferowanego systemu, jeżeli dla tego systemu funkcjonuje odpowiedni program certyfikacji lub szkoleń technicznych;
   II. posiadać doświadczenie w co najmniej jednym produkcyjnym wdrożeniu zaoferowanego produktu lub jego rodziny, zakończonym w okresie ostatnich 5 lat przed upływem terminu składania ofert;
   III. wykazać, że wdrożenie, o którym mowa w pkt 2, obejmowało integrację z co najmniej jednym z następujących rozwiązań lub mechanizmów: AD, LDAP, RADIUS, VPN lub logowanie Windows.
10) Endpoint Management - Osoba odpowiedzialna za Endpoint Management musi posiadać doświadczenie w co najmniej jednym produkcyjnym wdrożeniu zaoferowanego produktu lub jego rodziny, obejmującym:
   a. wdrożenie agentów;
   b. inventory;
   c. patch management;
   d. software deployment.

7.2. Podstawy wykluczenia Wykonawcy

Z postępowania wyklucza się Wykonawcę:

1) wobec którego zachodzą przesłanki wykluczenia, o których mowa w art. 5k rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. (w brzmieniu nadanym rozporządzeniem 2022/576);

2) wobec którego zachodzą przesłanki wykluczenia, o których mowa w 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;
3) powiązanego z Zamawiającym osobowo lub kapitałowo w sposób określony w Rozdziale 9 OPZ (konflikt interesów);
4) który w wyniku zawinionego działania lub zaniechania nienależycie wykonał wcześniejsze zamówienie na rzecz Zamawiającego w okresie ostatnich 3 lat przed upływem terminu składania ofert, co zostało stwierdzone prawomocnym orzeczeniem sądu, ostateczną decyzją administracyjną lub udokumentowane w inny wiarygodny sposób;
5) który nie wykazał spełnienia warunków udziału w postępowaniu określonych w pkt 7.1.

Na potwierdzenie braku podstaw wykluczenia wykonawca składa oświadczenia stanowiące Załącznik nr 3 i Załącznik nr 4 do zapytania ofertowego.

7.3. Przesłanki odrzucenia oferty

1. Zamawiający wezwie Wykonawcę do uzupełnienia oferty, która jest niekompletna - w terminie minimum 2 dni roboczych. Wyjaśnienia i uzupełnienia nie mogą prowadzić do zmiany ceny zaoferowanego przedmiotu zamówienia, deklaracji ocenianych w kryteriach oceny ofert ani zastąpienia zaoferowanego rozwiązania innym.
2. Zamawiający odrzuci w postępowaniu oferty Wykonawców, którzy w okresie ostatnich 3 lat od daty składania ofert nie podpisali umów z Zamawiającym w prowadzonych postępowaniach lub nienależycie wykonali zamówienie.
3. Zamawiający odrzuci ofertę, jeżeli obejmuje ona produkt ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 z późn. zm.), lub usługę ICT, lub proces ICT, określone w tej decyzji.

Rozdział 8: INFORMACJA O OŚWIADCZENIACH I DOKUMENTACH, JAKIE MAJĄ ZŁOŻYĆ WRAZ Z OFERTĄ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIENIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU:

Wykonawca załączy do oferty następujące dokumenty potwierdzające spełnienie warunków udziału w postępowaniu o udzielenie zamówienia:

1) Formularz oferty – załącznik nr 1 do zapytania ofertowego (podpisany elektronicznie);

2) Oświadczenie dotyczące podstaw wykluczenia i warunków udziału w postępowaniu – załącznik nr 3 do zapytania ofertowego (podpisany elektronicznie)
3) Oświadczenie Wykonawcy dotyczące przesłanek wykluczenia – załącznik nr 4 do zapytania ofertowego (podpisany elektronicznie)
4) Wykaz wykonanych dostaw/usług - załącznik nr 5 do zapytania ofertowego (podpisany elektronicznie)

   Zawiera wykaz usług wykonanych nie wcześniej niż w okresie ostatnich 3 lat przed terminem składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich rodzaju, wartości, daty i miejsca wykonania oraz podmiotów, na rzecz których dostawy te zostały wykonane, oraz załączeniem dowodów określających, czy te dostawy zostały wykonane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a jeżeli Wykonawca z przyczyn niezależnych od niego nie jest wstanie uzyskać tych dokumentów dopuszcza się złożenie oświadczenia Wykonawcy potwierdzającego należyte wykonanie usług, wraz ze wskazaniem przyczyn braku możliwości uzyskania referencji lub innych dokumentów od podmiotu, na rzecz którego usługi zostały wykonane.
5) Wykaz osób – załącznik nr 6 do zapytania ofertowego (podpisany elektronicznie)

   Zawiera wykaz osób skierowanych przez Wykonawcę do realizacji zamówienia publicznego, w szczególności odpowiedzialnych za wdrożenie rozwiązań objętych niniejszym przedmiotem zamówienia, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami sporządzonego zgodnie z załącznikiem nr 6 do zapytania ofertowego - w odniesieniu do warunku określonego w Rozdziale 7 OPZ.
6) Aktualny odpis z właściwego rejestru albo zaświadczenie o wpisie do ewidencji działalności gospodarczej.
7) Dokument potwierdzający, że Wykonawca jest ubezpieczony odpowiedzialności cywilnej w zakresie ubezpieczenie ryzyk cybernetycznych prowadzonej działalności na sumę gwarancyjną nie mniejszą niż 300 000,00.

8) Na potwierdzenie spełnienia warunku Wykonawca dostarczy zgodnie Rozdziałem 7 i 8 Zapytania ofertowego dowody należytego wykonanych dostaw/zamówień (referencje lub inne dokumenty stwierdzające należyte wykonanie).

Rozdział 9: KONFLIKT INTERESÓW, KLAUZULE ANTYKORUPCYJNE ORAZ WYKONAWCY WYSTĘPUJĄCY WSPÓLNIE

1. Konflikt interesów i zakaz powiązań

1) Zamawiający podejmuje środki, aby skutecznie zapobiegać konfliktom interesów, rozpoznawać je i likwidować, by zapewnić równe traktowanie Wykonawców.
2) W celu uniknięcia konfliktu interesów, zamówienie nie może być udzielone podmiotom powiązanym z Zamawiającym osobowo lub kapitałowo.
3) Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym (lub osobami upoważnionymi do zaciągania zobowiązań w jego imieniu) a Wykonawcą, polegające w szczególności na:
    - 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;
    - 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.
4) Każda osoba wykonująca czynności w postępowaniu składa (pod rygorem odpowiedzialności karnej) oświadczenie o braku powiązań z Wykonawcami, którzy złożyli oferty.

2. Klauzula antykorupcyjna

1) Wykonawca zobowiązuje się do podjęcia wszelkich niezbędnych środków w celu uniknięcia praktyk korupcyjnych. Za „praktyki korupcyjne” uznaje się oferowanie łapówek, upominków lub gratyfikacji jako zachęty za wykonanie lub powstrzymanie się od czynności związanych z udzieleniem zamówienia.
2) Wykonawca oświadcza, że:

- nie złożył i nie będzie oferować żadnych korzyści majątkowych w celu otrzymania zlecenia;
- nie brał i nie będzie brał udziału w zmowie z innymi Wykonawcami, aby w jakikolwiek sposób wpłynąć na proces wyboru.

3) Naruszenie klauzuli antykorupcyjnej może spowodować odrzucenie oferty lub przedterminowe wypowiedzenie umowy przez Zamawiającego.

3. Wykonawcy występujący wspólnie (Konsorcja)

1) Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania w postępowaniu i zawarcia umowy. Pełnomocnictwo należy dołączyć do oferty.
2) Wszelka korespondencja związana z postępowaniem kierowana będzie wyłącznie do ustanowionego pełnomocnika.
3) W przypadku wspólnego ubiegania się o zamówienie, oświadczenia o niepodleganiu wykluczeniu składa każdy z Wykonawców oddzielnie. Oświadczenia te potwierdzają brak podstaw wykluczenia u każdego z członków konsorcjum.
4) Warunki udziału w postępowaniu dotyczące zdolności technicznej lub zawodowej mogą być spełniane przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, z następującymi zastrzeżeniami:
   a) Warunek dotyczący doświadczenia we wdrażaniu rozwiązań cyberbezpieczeństwa, określony w Rozdziale 7 pkt 7.1 lit. c ppkt I oraz II.1–II.3 zapytania ofertowego, musi zostać spełniony w całości przez co najmniej jednego z Wykonawców wspólnie ubiegających się o zamówienie.
   b) Warunek dotyczący wykonania co najmniej dwóch audytów cyberbezpieczeństwa, określony w Rozdziale 7 pkt 7.1 lit. c ppkt II.4 zapytania ofertowego, musi zostać spełniony w całości przez co najmniej jednego z Wykonawców wspólnie ubiegających się o zamówienie, przy czym może to być inny Wykonawca niż wskazany w lit. a).
   c) Zamawiający nie dopuszcza sumowania pojedynczych realizacji różnych Wykonawców w celu osiągnięcia wymaganej liczby dwóch zamówień wdrożeniowych lub dwóch audytów cyberbezpieczeństwa w ramach danego warunku.

d) Wykonawcy, których doświadczenie jest wykazywane na potwierdzenie spełnienia warunków udziału w postępowaniu, zobowiązani są do rzeczywistego uczestnictwa w realizacji odpowiednich części zamówienia.

5) Jeżeli Wykonawcy ubiegają się o zamówienie wspólnie, są zobowiązani dołączyć do oferty oświadczenie, z którego wynika, które usługi/dostawy wykonają poszczególni Wykonawcy.

4. Podwykonawstwo

1) Wykonawca może powierzyć wykonanie części zamówienia Podwykonawcy.
2) Zamawiający żąda wskazania w ofercie części zamówienia, których wykonanie Wykonawca zamierza powierzyć podwykonawcom, oraz podania nazw firm podwykonawców (o ile są znani).
3) Powierzenie części zamówienia podwykonawcy nie zmienia zobowiązań Wykonawcy wobec Zamawiającego – Wykonawca pozostaje odpowiedzialny za należyte wykonanie całego zamówienia.

Rozdział 10: CENA OFERTY:

1. Cena winna uwzględniać wszelkie koszty Wykonawcy związane z realizacją zamówienia.
2. Wszelkie rozliczenia między Zamawiającym i Wykonawcą będą prowadzone w PLN.
3. Wykonawcy powinni zastosować stawkę podatku VAT od towarów i usług zgodną z ustawą o podatku VAT i podatku akcyzowym.

Rozdział 11: OPIS KRYTERIÓW KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY:

Oferty spełniające wymagania formalne określone w niniejszej instrukcji złożone przez Wykonawców nie podlegających wykluczeniu, będą oceniane według poniższych kryteriów i wag:

P = C + G

C - Cena oferty – 70%

W tym kryterium oferta może uzyskać max. 70 punktów

1 % odpowiada punktacji końcowej 1 pkt.

Sposób dokonywania oceny wg wzoru:

C = Cn : Cb x 70 pkt; gdzie:

Cn – cena najniższa,

Cb – cena badana

G – Przedłużona Gwarancja – 30 %

0 – punktów (%) za zaoferowanie 36 miesięcy gwarancji i wsparcia.

10 - punktów (%) za zaoferowanie 36 miesięcy gwarancji i wsparcia oraz gwarancji i bezpłatnego wsparcia w okresie kolejnych 12 miesięcy.

30 - punktów (%) za zaoferowanie 36 miesięcy gwarancji i wsparcia oraz gwarancji i bezpłatnego wsparcia w okresie kolejnych 24 miesięcy.

Gwarancja oraz przedłużona gwarancja

1. Wykonawca udziela gwarancji na dostarczony sprzęt, oprogramowanie, konfigurację, integrację oraz wdrożony system cyberbezpieczeństwa, na okres wymagany w dokumentacji zamówienia. Jeżeli Wykonawca zaoferuje przedłużony okres gwarancji, wszystkie obowiązki określone w niniejszym rozdziale obowiązują przez cały zaoferowany okres, na jednakowych zasadach.

2. Okres gwarancji i objętych nią usług utrzymania rozpoczyna się w dniu podpisania protokołu odbioru końcowego. Do tego dnia Wykonawca zapewnia ważność licencji, działanie wdrażanych rozwiązań oraz wsparcie w ramach realizacji zamówienia.

3. Przez cały okres gwarancji, w tym gwarancji przedłużonej, Wykonawca zapewnia, bez dodatkowych opłat dla Zamawiającego:

a) utrzymanie ważności wszystkich licencji, subskrypcji i uprawnień niezbędnych do zachowania funkcjonalności wymaganych w OPZ i zaoferowanych przez Wykonawcę;

b) odnawianie usług producentów, dostępu do aktualizacji, baz sygnatur, informacji o zagrożeniach oraz wsparcia producenta, jeżeli są niezbędne do prawidłowego działania i utrzymania oferowanych rozwiązań;

c) wsparcie techniczne, diagnostykę oraz usuwanie awarii, błędów, usterek i problemów dotyczących działania, konfiguracji oraz integracji systemu;

d) wykonywanie aktualizacji oprogramowania, systemów operacyjnych, firmware, komponentów bezpieczeństwa i baz sygnatur;

e) nadzór nad działaniem systemu, analizę alertów i zdarzeń bezpieczeństwa oraz podejmowanie działań w przypadku wykrycia nieprawidłowości;

f) reagowanie na wykryte lub zgłoszone ataki i incydenty cyberbezpieczeństwa dotyczące środowiska objętego zamówieniem;

g) utrzymanie i dostosowywanie konfiguracji zabezpieczeń w zakresie niezbędnym do zachowania wymaganej funkcjonalności i skuteczności ochrony;

h) aktualizację dokumentacji powykonawczej w zakresie wprowadzonych zmian.

4. Wykonawca zapewnia ciągłość obowiązywania licencji i subskrypcji, dokonując ich odnowienia przed upływem ważności. Niedopuszczalne jest ograniczenie funkcjonalności, przejście w tryb demonstracyjny, utrata aktualizacji lub wyłączenie mechanizmów ochrony wskutek nieodnowienia wymaganych uprawnień.

5. Wskazane w OPZ daty minimalnej ważności licencji, subskrypcji lub wsparcia, w szczególności 31 grudnia 2026 r., nie ograniczają obowiązku zapewnienia ich przez cały okres gwarancji oraz gwarancji przedłużonej. Jeżeli okres ten kończy się później, Wykonawca zapewnia odpowiednie przedłużenie na własny koszt.

6. Aktualizacje obejmują ich pozyskanie, ocenę kompatybilności, przygotowanie, instalację oraz sprawdzenie poprawności działania systemu po aktualizacji. Aktualizacje mogące wpływać na ciągłość pracy infrastruktury OT/ICS wykonuje się w uzgodnionych z Zamawiającym oknach serwisowych, po zabezpieczeniu konfiguracji i przygotowaniu sposobu przywrócenia poprzedniego stanu. W przypadku braku możliwości bezpiecznego zastosowania poprawki Wykonawca wdroży uzgodnione zabezpieczenia zastępcze i przedstawi plan usunięcia podatności.

7. Nadzór obejmuje co najmniej kontrolę dostępności i stanu komponentów, poprawności komunikacji i integracji, aktualności zabezpieczeń, ważności licencji oraz działania mechanizmów

rejestrowania i wykrywania zdarzeń. Monitoring automatyczny działa całodobowo. Bieżąca obsługa techniczna jest świadczona w dni robocze w godzinach 8:00–16:00, natomiast obsługa incydentów krytycznych odbywa się całodobowo, przez wszystkie dni tygodnia.

8. Reagowanie na incydenty obejmuje analizę zdarzenia, ocenę jego zakresu i skutków, powiadomienie Zamawiającego, ograniczenie rozprzestrzeniania zagrożenia, zabezpieczenie dostępnych dowodów, działania naprawcze oraz wsparcie przy przywracaniu bezpiecznego działania systemu. Działania ingerujące w procesy technologiczne wymagają uzgodnienia z upoważnionym przedstawicielem Zamawiającego, z uwzględnieniem wcześniej zatwierdzonych procedur reagowania.

9. W przypadku incydentu krytycznego, rozumianego jako aktywny atak lub zdarzenie powodujące albo bezpośrednio zagrażające utratą ciągłości usług, szyfrowaniem danych, nieuprawnionym dostępem administracyjnym lub utratą kluczowych mechanizmów ochrony, Wykonawca rozpocznie analizę i działania ograniczające zagrożenie w czasie nie dłuższym niż 1 godzina od wykrycia zdarzenia lub otrzymania zgłoszenia. Samo automatyczne potwierdzenie zgłoszenia nie stanowi rozpoczęcia reakcji.

10. Wykonawca zapewni jeden punkt kontaktu do zgłaszania problemów i incydentów oraz będzie prowadził rejestr zgłoszeń, podjętych działań i terminów ich realizacji. Co miesiąc przekaże Zamawiającemu raport obejmujący stan systemu, wykonane aktualizacje, obsłużone incydenty, ważność licencji i zalecane działania.

11. Wszystkie koszty realizacji powyższych obowiązków przez cały zaoferowany okres, w tym opłaty producentów, odnowienia licencji, robocizna, dojazdy oraz obsługa na miejscu, są dodatkową bezpłatną usługą, za która Wykonawca może otrzymać dodatkowe punkty w ocenie ofert. Wykonawca nie może uzależniać ich wykonania od zawarcia dodatkowej odpłatnej umowy, wykupienia pakietu serwisowego ani zakupu dodatkowych roboczogodzin. Limit roboczogodzin przewidziany dla usługi Managed Detection and Response (MDR) w OPZ nie ogranicza obowiązków wynikających z niniejszego rozdziału.

12. Wykonawca odpowiada wobec Zamawiającego za całość obsługi, również gdy korzysta ze wsparcia producentów lub podwykonawców. Zdalny dostęp serwisowy wymaga autoryzacji, stosowania bezpiecznych mechanizmów dostępu oraz rejestrowania wykonywanych czynności.

13. Obowiązki obejmują środowisko dostarczone i objęte wdrożeniem. Rozbudowa o nowe lokalizacje, urządzenia lub użytkowników ponad zakres zamówienia wymaga odrębnych ustaleń. Usunięcie błędów wdrożenia, utrzymanie wymaganej funkcjonalności i obsługa incydentów w istniejącym zakresie nie stanowią rozbudowy.

Rozdział 12: TERMIN SKŁADANIA OFERT:

1. Ofertę wraz z niezbędnymi załącznikami należy złożyć za pośrednictwem Bazy Konkurencyjności (BK2021), dostępnej pod adresem: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/
2. Ofertę wraz z wymaganymi załącznikami należy złożyć w terminie **do dnia 20.11.2026 roku.**
3. Wykonawca może złożyć tylko jedną ofertę.
4. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.

Rozdział 13: TERMIN OTWARCIA OFERT:

1. Otwarcie ofert nastąpi w dniu **23.11.2026 roku o godzinie 9:00.**
2. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o:
   1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania Wykonawców, których oferty zostały otwarte;
   2) cenach lub kosztach zawartych w ofertach.
3. W przypadku wystąpienia awarii systemu teleinformatycznego, która spowoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
4. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.

Rozdział 14: UNIEWAŻNIENIE POSTĘPOWANIA:

1. Zamawiający może unieważnić postępowanie przed zawarciem umowy, jeżeli:
    a) nie złożono żadnej oferty w terminie składania ofert;
    b) wszystkie złożone oferty podlegają odrzuceniu zgodnie z zasadami określonymi w zapytaniu ofertowym;
    c) cena najkorzystniejszej oferty przewyższa kwotę, którą Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia, chyba że Zamawiający może zwiększyć tę kwotę do ceny najkorzystniejszej oferty;
    d) postępowanie obarczone jest niemożliwą do usunięcia wadą uniemożliwiającą zawarcie ważnej umowy lub udzielenie zamówienia zgodnie z zasadą konkurencyjności, w szczególności z zasadami uczciwej konkurencji, równego traktowania wykonawców i przejrzystości;
    e) środki przeznaczone na sfinansowanie zamówienia nie zostały przyznane, zostały cofnięte lub zmniejszone, a Zamawiający nie ma możliwości sfinansowania zamówienia z innych środków;
    f) wystąpiła istotna zmiana okoliczności, której nie można było przewidzieć w chwili wszczęcia postepowania, powodująca, że dalsze prowadzenie postępowania lub wykonanie zamówienia nie służy realizacji uzasadnionych potrzeb Zamawiającego albo celów projektu;
    g) wybrany Wykonawca uchyla się od zawarcia umowy lub nie spełnia określonych w zapytaniu ofertowym warunków jej zawarcia, a wybór kolejnej oferty zgodnie z zasadami postępowania nie jest możliwy;
    h) unieważnienie postepowania wymaga uzasadnienia wskazującego podstawę określoną w ust. 1 oraz konkretne okoliczności faktyczne uzasadniające podjętą decyzję. Decyzja nie może mieć charakteru arbitralnego ani naruszać zasad uczciwej konkurencji, równego traktowania wykonawców i przejrzystości;
    i) informację o unieważnieniu postępowania, wraz z uzasadnieniem, Zamawiający niezwłocznie publikuje na stronie ogłoszenie w Bazie Konkurencyjności (BK2021). Jeżeli unieważnienie następuje po upływie terminu ofert, Zamawiający przekazuje tę informację również Wykonawcom, którzy złożyli oferty, na adres poczty elektronicznej wskazane w ofertach.

j) Decyzje o unieważnieniu postępowania wraz z uzasadnieniem Zamawiający dołącza do dokumentacji postępowania.

Rozdział 15: ZOBOWIĄZANIA WYKONAWCY ZWIĄZANE Z UMOWĄ:

1. Zostały określone w projekcie umowy i Opisie Przedmiotu Zamówienia.
2. Umowa zostanie zawarta w formie pisemnej, w terminie nie krótszym niż 7 dni od dnia przekazania informacji o wyborze oferty.
3. Zamawiający może zawrzeć umowę przed upływem terminu określonego w ust. 2, jeżeli w postępowaniu o udzielenie zamówienia złożono tylko jedną ofertę.

Rozdział 16: WADIUM

1. Wykonawca przystępujący do postępowania zobowiązany jest do wniesienia wadium w wysokości: 10 000,00 złotych (słownie: dziesięć tysięcy złotych)
2. Wadium można wnieść w pieniądzu, poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, gwarancjach bankowych, gwarancjach ubezpieczeniowych. Wadium wnoszone w pieniądzu należy wpłacić na rachunek: **86 1240 5787 1111 0010 7723 9223.** Oryginał dokumentu (gwarancji, poręczenia itp.) należy dołączyć do oferty. Do ofert należy dołączyć dowód wniesienia wadium, o którym mowa w pkt. 1 lub kopię potwierdzenia dokonania przelewu – w przypadku wniesienia wadium w pieniądzu.
3. Zamawiający niezwłocznie zwraca wadium, jeżeli:
    1) upłynął termin związania ofertą,
    2) zawarto umowę,
    3) unieważniono postępowanie, a protesty zostały ostatecznie rozstrzygnięte lub upłynął termin ich wniesienia,
    4) Wykonawcy, który wycofał ofertę przed upływem terminu składania ofert – niezwłocznie po złożeniu pisemnego wniosku o zwrot wadium,
    5) Wykonawcy, który został wykluczony z postępowania bądź którego oferta została odrzucona – niezwłocznie po złożeniu pisemnego wniosku o zwrot wadium, przy czym

złożenie takiego wniosku jest równoznaczne ze zrzeczeniem się przez Wykonawcę prawa do wniesienia sprzeciwu.

4. Jeżeli wadium wniesiono w pieniądzu, Zamawiający zwraca je na wskazany rachunek Wykonawcy, po otrzymaniu wniosku z podaniem numeru konta na które ma być zwrócone.

1) Wadium przechowywanie jest na nieoprocentowanym rachunku.

5. Zamawiający zatrzymuje wadium, jeżeli Wykonawca, którego oferta została wybrana:
   1) odmówił podpisania umowy na warunkach określonych w ofercie,
   2) zawarcie umowy stało się niemożliwe z przyczyn leżących po stronie Wykonawcy.
   3) Wykonawca w odpowiedzi na wezwanie do uzupełnienia oferty nie złożył dokumentów lub oświadczeń potwierdzających spełnienie warunków udziału w postępowaniu albo pełnomocnictw, chyba że udowodni, że wynika to z przyczyn nieleżących po jego stronie.

Rozdział 17: ZASADY SKŁADANIA ODWOŁAŃ:

1. Odwołanie przysługuje Wykonawcom, wyłącznie od niezgodnej z przepisami czynności Zamawiającego podjętej w postępowaniu o udzielenie zamówienia lub zaniechania czynności, do której Zamawiający jest zobowiązany na podstawie Regulaminu.
2. Odwołanie wnosi się do Zamawiającego w formie pisemnej w terminie 3 dni od dnia doręczenia informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia.
3. Wniesienie odwołania jest dopuszczalne tylko przed zawarciem umowy przez Zamawiającego. Odwołanie wnosi się wyłącznie w formie pisemnej podając uzasadnienie jego wniesienia.
4. Odwołanie powinno wskazywać zaskarżoną czynność lub zaniechanie Zamawiającego, której zarzuca się niezgodność z przepisami regulaminu, zawierać zwięzłe przedstawienie zarzutów, określać żądanie oraz wskazywać faktyczne i prawne uzasadnienie odwołania.
5. W przypadku wniesienia skargi dotyczącej treści ogłoszenia lub postanowień OPZ Zamawiający może przedłużyć termin składania ofert.
6. Informację o wniesieniu skargi wraz z jej kopią Zamawiający przekazuje pozostałym Wykonawcom uczestniczącym w postępowaniu o udzielenie zamówienia, a jeżeli skarga dotyczy treści ogłoszenia lub postanowień OPZ, zamieszcza ja również na stronie internetowej, na której jest udostępniany Opis przedmiotu Zamówienia.
7. Do czasu rozstrzygnięcia Zamawiający nie może zawrzeć umowy.

8. Odwołanie rozstrzyga się w terminie 5 dni od daty jego wniesienia.
9. Rozpatrując odwołanie Zamawiający może je uwzględnić lub odrzucić.
10. Rozstrzygnięcie skargi wraz z uzasadnieniem Zamawiający przekazuje jednocześnie podmiotowi, który wniósł skargę oraz pozostałym Wykonawcom uczestniczącym w postępowaniu o udzielenie zamówienia, a jeżeli skarga dotyczy treści ogłoszenia lub postanowień OPZ, zamieszcza ją również na stronie internetowej, na której jest udostępniony OPZ.
11. W przypadku uwzględnienia skargi Zamawiający powtarza skarżoną czynność.
12. O powtórzeniu czynności Zamawiający informuje niezwłocznie wszystkich Wykonawców.
13. Od decyzji Zamawiającego rozstrzygającej odwołanie nie przysługują dalsze środki odwoławcze.

Rozdział 18: OGŁOSZENIE WYNIKÓW POSTĘPOWANIA:

Informacje o rozstrzygnięciu postępowania zostaną zamieszczone za pośrednictwem platformy zakupowej Baza Konkurencyjności pod adresem:
https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/

Rozdział 19: KLAUZULA INFORMACYJNA DOTYCZĄCA PRZETWARZANIA DANYCH OSOBOWYCH.

Zgodnie z art. 13 ust.1 i 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

a) Administratorem Pani/Pana danych osobowych jest Zakład Usług Gminnych Gmina Ełk Sp. z o.o. z siedzibą w Ełku (19-300) ul. T. Kościuszki 28A;
b) Administrator powołał Inspektora Ochrony Danych Osobowych; kontakt do IOD: iod@elk.gmina.pl ; Telefon: 87 619 45 50
c) Pani/Pana dane osobowe będą przetwarzane na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego w ramach

projektu pn. „Poprawa cyberbezpieczeństwa w Zakładzie Usług Gminnych Gmina Ełk Sp. z o.o.”

d) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o przepisy ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. 2021 poz. 1129(, dalej „ustawa Pzp”;

e) Pani/Pana dane osobowe będą przechowywane przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;

f) obowiązek podania przez Panią/Pana danych osobowych jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;

g) Posiada Pani/Pan na podstawie art. 15 RODO prawo dostępu do swoich danych osobowych, na podstawie art. 16 RODO prawo do sprostowania swoich danych osobowych,

h) W razie naruszeń ochrony Pani/Pana danych osobowych, ma Pani/Pani prawo do złożenia skargi do organu nadzorczego – Urzędu Ochrony Danych Osobowych.

Signature Not Verified
Dokument podpisany przez Krzysztof Kurzynowski
Data: 2026.11.13 10:55:40 CET

Załączniki:

1. Formularz oferty – załącznik nr 1 do zapytania ofertowego;
2. Opis Przedmiotu Zamówienia (OPZ) - załącznik nr 2 do zapytania ofertowego;
3. Oświadczenie dotyczące podstaw wykluczenia i warunków udziału w postępowaniu – załącznik nr 3 do zapytania ofertowego;
4. Oświadczenie Wykonawcy dotyczące przesłanek wykluczenia – załącznik nr 4 do zapytania ofertowego;
5. Wykaz wykonanych dostaw, usług - załącznik nr 5 do zapytania ofertowego
6. Wykaz osób – załącznik nr 6 do zapytania ofertowego;
7. Projekt umowy – załącznik nr 7 do zapytania ofertowego.