Ogłoszenie o zamówieniu
Usługi
„Cyberbezpieczne Wodociągi - usługi wdrożeniowe i bezpieczeństwa IT dla Zakładu Gospodarki Komunalnej, Mieszkaniowej i Wodociągów w Niechlowie”

SEKCJA I - ZAMAWIAJĄCY

1.1.) Rola zamawiającego

Postępowanie prowadzone jest samodzielnie przez zamawiającego

1.2.) Nazwa zamawiającego: Zakład Gospodarki Komunalnej Mieszkaniowej i Wodociągów w Niechlowie

1.4) Krajowy Numer Identyfikacyjny: REGON 410210355

1.5) Adres zamawiającego

1.5.1.) Ulica: Szkolna 23

1.5.2.) Miejscowość: Niechlów

1.5.3.) Kod pocztowy: 56-215

1.5.4.) Województwo: dolnośląskie

1.5.5.) Kraj: Polska

1.5.6.) Lokalizacja NUTS 3: PL516 - Legnicko-głogowski

1.5.9.) Adres poczty elektronicznej: zamowieniapubliczne@niechlow.pl

1.5.10.) Adres strony internetowej zamawiającego: niechlow.zakladkomunalny.com

1.6.) Rodzaj zamawiającego: Zamawiający sektorowy - art. 5 ust. 1 pkt 1 - gospodarka wodna

1.7.) Przedmiot działalności zamawiającego: Inna działalność

Zaopatrzenie w wodę, odprowadzanie ścieków

SEKCJA II – INFORMACJE PODSTAWOWE

2.1.) Ogłoszenie dotyczy:

Zamówienia publicznego

2.2.) Ogłoszenie dotyczy usług społecznych i innych szczególnych usług: Nie

2.3.) Nazwa zamówienia albo umowy ramowej:

„Cyberbezpieczne Wodociągi - usługi wdrożeniowe i bezpieczeństwa IT dla Zakładu Gospodarki Komunalnej, Mieszkaniowej i Wodociągów w Niechlowie”

2.4.) Identyfikator postępowania: ocds-148610-2bc39844-caf5-4d28-a494-57eb7126c503

2.5.) Numer ogłoszenia: 2026/BZP 00533290

2.6.) Wersja ogłoszenia: 01

2.7.) Data ogłoszenia: 2026-11-10

2.8.) Zamówienie albo umowa ramowa zostały ujęte w planie postępowań: Nie

2.11.) O udzielenie zamówienia mogą ubiegać się wyłącznie wykonawcy, o których mowa w art. 94 ustawy: Nie

2.14.) Czy zamówienie albo umowa ramowa dotyczy projektu lub programu współfinansowanego ze środków Unii Europejskiej: Tak

2.15.) Nazwa projektu lub programu

Krajowy Plan Odbudowy i Zwiększania Odporności (KPO), Komponent C - Transformacja cyfrowa, Inwestycja C3.1.1. Cyberbezpieczeństwo - CyberPL, Konkurs Grantowy „Cyberbezpieczne Wodociągi”, nabór nr KPOD.05.10-CW.01-001/25, umowa o powierzenie grantu nr KPOD.05.10-CW.01-001/25/0737/KPOD.05.10-CW.01-001/25/2026

2.16.) Tryb udzielenia zamówienia wraz z podstawą prawną

Zamówienie udzielane jest w trybie podstawowym na podstawie: art. 275 pkt 1 ustawy

SEKCJA III – UDOSTĘPNIANIE DOKUMENTÓW ZAMÓWIENIA I KOMUNIKACJA

3.1.) Adres strony internetowej prowadzonego postępowania
https://niechlow.ezamawiajacy.pl/pn/niechlow/demand/336134/notice/public/details

3.2.) Zamawiający zastrzega dostęp do dokumentów zamówienia: Nie

3.4.) Wykonawcy zobowiązani są do składania ofert, wniosków o dopuszczenie do udziału w postępowaniu, oświadczeń oraz innych dokumentów wyłącznie przy użyciu środków komunikacji elektronicznej: Tak

3.5.) Informacje o środkach komunikacji elektronicznej, przy użyciu których zamawiający będzie komunikował się z wykonawcami - adres strony internetowej: W niniejszym postępowaniu komunikacja zamawiającego z wykonawcami odbywa się za pomocą środków komunikacji elektronicznej.
2. Pytania do SWZ należy zadawać za pośrednictwem platformy zakupowej zamawiającego przez link: https://niechlow.ezamawiajacy.pl. Instrukcja korzystania z systemu jest dostępna pod wyżej wskazanym adresem.
3. Oferta wraz z załącznikami musi być złożona w postaci elektronicznej w systemie informatycznym dostępnym pod adresem: https://niechlow.ezamawiajacy.pl/pn/niechlow/demand/336134/notice/public/details

3.6.) Wymagania techniczne i organizacyjne dotyczące korespondencji elektronicznej: Wymagania dotyczące zasad rejestracji oraz minimalnych parametrów technicznych wymaganych od wykonawcy przy wykorzystywaniu systemu do elektronicznej komunikacji z wykonawcami. Oferta wraz z załącznikami musi zostać złożona w postaci elektronicznej. Złożenie oferty wymaga do Wykonawcy zarejestrowania się i zalogowania w systemie informatycznym dostępnym pod adresem https://niechlow.ezamawiajacy.pl, zgodnie z poniższą
kolejnością. Rejestracja wykonawcy trwa maksymalnie do 2 dni roboczych. Mając to na uwadze, zamawiający zaleca wykonawcom uwzględnienie czasu niezbędnego na rejestrację w procesie złożenia oferty w postaci elektronicznej. Wykonawca po wybraniu opcji „przystąp do postępowania” zostanie przekierowany do strony https://oneplace.marketplanet.pl, gdzie zostanie powiadomiony o możliwości zalogowania lub do założenia bezpłatnego konta. Wykonawca biorący udział w postępowaniu prowadzonym drogą elektroniczną w systemie zakłada konto, wykonując kroki procesu rejestracyjnego; podaje adres e-mail, ustanawia hasło, następnie powtarza hasło, wpisuje kod z obrazka, akceptuje regulamin, klika polecenie „zarejestruj się”. Po założeniu konta wykonawca ma możliwość złożenia oferty w postępowaniu. Zamawiający wskazuje informacje, o których mowa w Rozporządzenia Prezesa Rady Ministrów w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępnienia i przechowywania dokumentów elektronicznych, dotyczące systemu dostępnego pod adresem https://niechlow.ezamawiajacy.pl:
• komputer PC/MAC z aktualnym systemem operacyjnym wspieranym przez producenta
• Wybrana przeglądarka wspierana przez producenta: MS Internet Explorer, Firefox, Google Chrome lub MS Edge
• Podłączenie do Internetu: min. 512 Kb/s na komputer (zalecane szerokopasmowe łącze internetowe);

3.7.) Adres strony internetowej, pod którym są dostępne narzędzia, urządzenia lub formaty plików, które nie są ogólnie dostępne: https://niechlow.ezamawiajacy.pl

3.8.) Zamawiający wymaga sporządzenia i przedstawienia ofert przy użyciu narzędzi elektronicznego modelowania danych budowlanych lub innych podobnych narzędzi, które nie są ogólnie dostępne: Nie

3.12.) Oferta - katalog elektroniczny: Nie dotyczy

3.14.) Języki, w jakich mogą być sporządzane dokumenty składane w postępowaniu:

polski

3.15.) RODO (obowiązek informacyjny): Klauzula informacyjna o przetwarzaniu danych została zawarta w rozdziale XXI SWZ

3.16.) RODO (ograniczenia stosowania): Klauzula informacyjna o przetwarzaniu danych została zawarta w rozdziale XXI SWZ

SEKCJA IV – PRZEDMIOT ZAMÓWIENIA

4.1.) Informacje ogólne odnoszące się do przedmiotu zamówienia.

4.1.1.) Przed wszczęciem postępowania przeprowadzono konsultacje rynkowe: Nie

4.1.2.) Numer referencyjny: ZGK.271.6.2026

4.1.3.) Rodzaj zamówienia: Usługi

4.1.4.) Zamawiający udziela zamówienia w częściach, z których każda stanowi przedmiot odrębnego postępowania: Nie

4.1.8.) Możliwe jest składanie ofert częściowych: Tak

4.1.9.) Liczba części: 6

4.1.10.) Ofertę można składać na wszystkie części

4.1.11.) Zamawiający ogranicza liczbę części zamówienia, którą można udzielić jednemu wykonawcy: Nie

4.1.13.) Zamawiający uwzględnia aspekty społeczne, środowiskowe lub etykiety w opisie przedmiotu zamówienia: Nie

4.2. Informacje szczegółowe odnoszące się do przedmiotu zamówienia:

Część 1

4.2.2.) Krótki opis przedmiotu zamówienia

3.1. Przedmiot. Wdrożenie systemu klasy SIEM opartego na oprogramowaniu Wazuh (lub równoważnym) jako centralnego systemu zbierania, korelacji i analizy zdarzeń bezpieczeństwa z systemów IT Zamawiającego, wraz z regułami, pulpitami, powiadamianiem, dokumentacją i instruktażem. Zamówienie obejmuje zakres podstawowy oraz zakres objęty prawem opcji.
3.2. Zakres podstawowy:
1) instalacja i konfiguracja serwera SIEM (komponenty zarządzania, indeksowania i wizualizacji) na maszynie wirtualnej platformy wirtualizacji Zamawiającego (udostępnianej w Części 2), w architekturze jednowęzłowej, z szyfrowaną komunikacją agentów, uwierzytelnianiem użytkowników z rolami (administrator, analityk, tylko odczyt) i kopią konfiguracji;
2) retencja zdarzeń: dane indeksowane dostępne do przeszukiwania przez co najmniej 90 dni, archiwum zdarzeń przez co najmniej 12 miesięcy na zasobach wskazanych przez Zamawiającego (macierz S16 lub NAS S21);
3) instalacja agentów na wszystkich stacjach roboczych i serwerach Zamawiającego (około 25 agentów: stacje robocze Windows, kontroler domeny, serwer plików, serwery platformy wirtualizacji i kopii zapasowych, maszyny wirtualne wdrażane w Częściach 2 i 3, stacja przesiadkowa S35), z grupami agentów i scentralizowaną konfiguracją;
4) integracja źródeł bez agenta przez syslog lub API: zapora sieciowa Stormshield, dwa przełączniki Cisco Catalyst 9200L, urządzenia QNAP (S16, S21), platforma wirtualizacji, serwer kopii zapasowych, serwer RADIUS, jeżeli zostanie uruchomiony do czasu odbioru;
5) zbieranie i analiza zdarzeń Active Directory: logowania udane i nieudane, blokady kont, tworzenie i modyfikacja kont i grup uprzywilejowanych, zmiany polityk, użycie kont administracyjnych;
6) monitorowanie integralności plików (FIM) na kontrolerze domeny, serwerze plików i serwerach platformy w katalogach uzgodnionych z Zamawiającym oraz ocena konfiguracji (SCA) serwerów według wzorców CIS dostępnych w oprogramowaniu;
7) reguły i alerty: co najmniej 20 reguł korelacyjnych lub progowych dopasowanych do środowiska Zamawiającego, w tym: wielokrotne nieudane logowania, logowanie poza godzinami pracy, użycie konta administracyjnego, nowe konto uprzywilejowane, zmiana polityki, agent niedostępny, zmiana plików krytycznych, wykrycie oprogramowania złośliwego, zdarzenia zapory o wysokim priorytecie, zmiana konfiguracji przełącznika, nieudane logowania do urządzeń QNAP i platformy wirtualizacji, uruchomienie i zakończenie sesji na stacji przesiadkowej; poziomy ważności i wyciszanie fałszywych alarmów;
8) powiadomienia o alertach o wysokim priorytecie pocztą elektroniczną na adresy wskazane przez Zamawiającego, z dziennym podsumowaniem zdarzeń;
9) co najmniej trzy pulpity: przegląd bezpieczeństwa, uwierzytelnianie i konta, integralność i zgodność; raport miesięczny generowany z systemu w formacie PDF;
10) stacja przesiadkowa S35: agent SIEM oraz przekazywanie do SIEM zdarzeń rozpoczęcia i zakończenia sesji administracyjnych z identyfikacją użytkownika i celu połączenia;
11) praca produkcyjna systemu przez co najmniej 5 dni kalendarzowych bez przerw z przyczyn leżących po stronie Wykonawcy przed zgłoszeniem gotowości do odbioru, ze zbieraniem zdarzeń z co najmniej 80 procent agentów i wszystkich źródeł bez agenta, z pierwszym dostrojeniem reguł na podstawie zebranych zdarzeń; okres liczy się od uruchomienia serwera SIEM na maszynie docelowej, a zalicza się do niego pracę w środowisku tymczasowym, jeżeli konfiguracja i zebrane zdarzenia zostały przeniesione na maszynę docelową; przerwy spowodowane przez Zamawiającego lub innych wykonawców nie przerywają biegu okresu;
12) dokumentacja według pkt 2.4, w tym opis reguł i instrukcja reagowania na poszczególne alerty, oraz instruktaż według pkt 2.5.
3.3. Zakres objęty prawem opcji (pakiet rozszerzony):
1) integracja z skanerem podatności (Część 2): import wyników skanów do SIEM i reguły alertujące o podatnościach krytycznych na aktywach;
2) integracja z systemem monitoringu (Część 2): przekazywanie alertów dostępności do SIEM i korelacja z zdarzeniami bezpieczeństwa;
3) zbieranie zdarzeń z punktów styku z siecią OT wskazanych przez Zamawiającego (serwer RADIUS sieci przemysłowej, przemysłowy przełącznik zarządzalny, bastion serwisowy OT) z regułami dla nieautoryzowanego dostępu do sieci przemysłowej;
4) dodatkowe strojenie reguł: 16 godzin prac analityka na podstawie zdarzeń z pracy produkcyjnej, wykonane po pierwszym dostrojeniu, o którym mowa w pkt 3.2 pkt 11, przed odbiorem części;
5) dodatkowy instruktaż dla administratora i Pełnomocnika ds. SZBI (6 godzin) z analizy alertów i obsługi incydentów w SIEM, prowadzony na zdarzeniach z pracy produkcyjnej.
3.4. Prawo opcji. Zamawiający może skorzystać z prawa opcji w całości, składając Wykonawcy oświadczenie w terminie do 11 grudnia 2026 r.; Zamawiający korzysta z opcji tylko wtedy, gdy w tym dniu platforma wirtualizacji z maszynami wirtualnymi (pkt 4.2) jest uruchomiona, a wdrożenia skanera podatności i monitoringu (pkt 4.4 i 4.5) są w toku zgodnie z harmonogramem, tak aby integracje z pkt 3.3 pkt 1 i 2 były wykonalne do 21 grudnia 2026 r. Skorzystanie z prawa opcji nie wymaga aneksu. Cały zakres opcjonalny wykonuje się w terminie wykonania Części 1 i odbiera razem z zakresem podstawowym. Nieskorzystanie z prawa opcji nie rodzi po stronie Wykonawcy żadnych roszczeń.
3.5. Zależności i termin. Maszynę wirtualną dla SIEM udostępnia Zamawiający (Część 2) nie później niż 11 grudnia 2026 r.;

do tego czasu Wykonawca przygotowuje konfigurację w środowisku tymczasowym (własnym lub udostępnionym przez Zamawiającego) i wykonuje prace niewymagające docelowej maszyny (agenty, integracje źródeł, reguły). Harmonogram graniczny: maszyna docelowa 11 grudnia, przeniesienie konfiguracji i rozpoczęcie pracy produkcyjnej 11 grudnia, co najmniej 5 dni kalendarzowych pracy produkcyjnej do 16 grudnia, zawiadomienie o planowanym odbiorze 16 grudnia, zgłoszenie wykonania po zakończeniu wszystkich prac (w tym opcji), nie później niż 21 grudnia, odbiór i protokół 21 grudnia albo następnego dnia roboczego; integracje objęte opcją (pkt 3.3 pkt 1 i 2) wymagają uruchomienia skanera i monitoringu w Części 2 do 15 grudnia. Jeżeli maszyna zostanie udostępniona później, termin wykonania Części 1 może zostać przedłużony aneksem o liczbę dni opóźnienia, nie dalej jednak niż do 23 grudnia 2026 r., na zasadach określonych w umowie; Wykonawca nie ponosi odpowiedzialności za opóźnienie z tej przyczyny.
3.6. Testy odbiorowe: sprawdzenie liczby i stanu agentów; wygenerowanie zdarzeń testowych (nieudane logowania do domeny, utworzenie konta testowego i nadanie uprawnień, modyfikacja monitorowanego pliku, zdarzenie testowe z zapory i z przełącznika, sesja testowa ze stacji przesiadkowej) i potwierdzenie alertów oraz powiadomień; przegląd pulpitów i raportu; odtworzenie konfiguracji z kopii; w przypadku opcji - potwierdzenie importu wyników skanu i alertu z systemu monitoringu.

4.2.6.) Główny kod CPV: 72000000-5 - Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

4.2.7.) Dodatkowy kod CPV:

72263000-6 - Usługi wdrażania oprogramowania

72250000-2 - Usługi w zakresie konserwacji i wsparcia systemów

72220000-3 - Usługi doradcze w zakresie systemów i doradztwo techniczne

72800000-8 - Usługi audytu komputerowego i testowania komputerów

72600000-6 - Usługi doradcze i dodatkowe w zakresie sprzętu komputerowego

4.2.8.) Zamówienie obejmuje opcje: Tak

4.2.9) Rodzaj i maksymalna wartość opcji oraz okoliczności skorzystania z opcji:
Zamawiający może skorzystać z prawa opcji obejmującego pakiet rozszerzony określony w pkt 3.3 SOPZ, składając wykonawcy oświadczenie w terminie do 11 grudnia 2026 r. Zakres opcjonalny jest wyceniany odrębnie w formularzu ofertowym, a jego cena wchodzi do ceny oferty podlegającej ocenie. Zakres opcjonalny jest wykonywany i odbierany razem z zakresem podstawowym w terminie wykonania Części 1. Nieskorzystanie z prawa opcji nie rodzi roszczeń wykonawcy.

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: do 2026-12-21

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert:

4.3.1.) Sposób oceny ofert: Zamawiający wybiera najkorzystniejszą ofertę na podstawie kryteriów oceny ofert. Oferta złożona przez Wykonawcę może otrzymać łącznie 100 pkt.

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Punktowo

4.3.3.) Stosowane kryteria oceny ofert: Kryterium ceny oraz kryteria jakościowe

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 60

Kryterium 2

4.3.4.) Rodzaj kryterium: serwis posprzedażny, pomoc techniczna, warunki dostawy takich jak termin, sposób lub czas dostawy, oraz okresu realizacji.

4.3.5.) Nazwa kryterium: „Okres Wsparcia Po Odbiorze”

4.3.6.) Waga: 40

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

Część 2

4.2.2.) Krótki opis przedmiotu zamówienia

CZĘŚĆ 2 - PLATFORMA WIRTUALIZACJI, KOPIE ZAPASOWE, MONITORING I SKANER PODATNOŚCI
4.1. Przedmiot. Wdrożenie platformy wirtualizacji Proxmox VE na serwerze S13, systemu kopii zapasowych na serwerze S14 z repliką na NAS S21, systemu monitoringu Zabbix oraz skanera podatności Greenbone/OpenVAS (lub rozwiązań równoważnych), wraz z dokumentacją i instruktażem.
4.2. Platforma wirtualizacji:
1) instalacja Proxmox VE na serwerze S13 z wykorzystaniem dostarczonej konfiguracji dyskowej (sprzętowy RAID albo pula ZFS na kontrolerze HBA, zależnie od dostarczonego serwera), oddzielenie dysków systemowych od przestrzeni na maszyny wirtualne, podłączenie macierzy S16 jako magazynu (iSCSI lub NFS, zgodnie z możliwościami urządzenia, z wielościeżkowością, jeżeli jest dostępna);
2) konfiguracja sieci platformy: mostki, VLAN-y zgodne z projektem architektury (Część 4) lub ustaleniami z Zamawiającym, odseparowany interfejs zarządzania, łącza 10 GbE do przełączników, agregacja łączy, jeżeli przełączniki ją obsługują;
3) utrzymanie dostępu administracyjnego wyłącznie z sieci zarządzania i stacji przesiadkowej, uwierzytelnianie dwuskładnikowe dla kont administracyjnych platformy, aktualizacje z repozytorium bez subskrypcji, kopia konfiguracji hosta;
4) utworzenie i przekazanie maszyn wirtualnych z systemem operacyjnym Linux LTS, utwardzonych (aktualizacje, zapora systemowa, konta imienne, logowanie kluczem) dla: SIEM (Część 1; zasoby co najmniej 8 vCPU, 32 GB RAM, 1 TB przestrzeni), Zabbix, skanera podatności, GLPI (Część 3) oraz jednej maszyny rezerwowej według wskazań Zamawiającego; maszyna dla SIEM udostępniona nie później niż 11 grudnia 2026 r.;
5) migracja maszyn wirtualnych lub systemów wskazanych przez Zamawiającego nie wchodzi w zakres zamówienia; Wykonawca przekazuje Zamawiającemu procedurę tworzenia i migracji maszyn.
4.3. Kopie zapasowe:
1) instalacja Proxmox Backup Server na serwerze S14 z magazynem kopii na jego dyskach, integracja z platformą, zadania kopii wszystkich maszyn wirtualnych z harmonogramem codziennym, deduplikacją, weryfikacją kopii i retencją uzgodnioną z Zamawiającym (co najmniej 14 kopii dziennych, 4 tygodniowe, 3 miesięczne);
2) druga kopia na NAS S21: synchronizacja magazynu kopii na odrębny magazyn na NAS z własnym harmonogramem i retencją, z ochroną przed modyfikacją (migawki lub tryb tylko do odczytu), tak aby po utracie serwera S14 możliwe było odtworzenie maszyn z NAS;
3) powiadomienia o wyniku zadań kopii, test odtworzenia maszyny wirtualnej z kopii na serwerze S14 oraz z kopii na NAS przy niedostępnym serwerze S14, udokumentowany protokołem;
4) kopia konfiguracji przełączników, zapory i urządzeń QNAP do magazynu kopii, jeżeli urządzenia to umożliwiają, w uzgodnieniu z ASI.
4.4. System monitoringu:
1) instalacja Zabbix na maszynie wirtualnej; objęcie monitoringiem: serwerów S13 i S14 (agent i interfejs zarządzania sprzętowego), urządzeń QNAP, przełączników, zapory sieciowej, kontrolera domeny i serwera plików, zasilaczy UPS z kartami sieciowymi, dostępności łączy do obiektów technologicznych (test dostępności bez ingerencji w sieć OT), maszyn wirtualnych;
2) szablony, progi i wyzwalacze dla dostępności, obciążenia, przestrzeni dyskowej, temperatury i stanu zasilania, stanu macierzy i kopii zapasowych; mapa sieci; pulpit stanu infrastruktury;
3) powiadomienia pocztą elektroniczną oraz możliwość przekazywania alertów do SIEM (realizowana w ramach opcji Części 1).
4.5. Skaner podatności:
1) instalacja Greenbone Community Edition (OpenVAS) na maszynie wirtualnej z aktualnym zestawem testów, cele skanowania: sieć biurowa, serwery, maszyny wirtualne, urządzenia sieciowe, z wyłączeniem sieci OT;
2) harmonogram skanów tygodniowych w oknie uzgodnionym z Zamawiającym, uwierzytelnione skany serwerów Linux, raporty w formacie PDF i w formacie umożliwiającym import do SIEM;
3) skan bazowy z raportem zawierającym podatności według ważności i zalecenia usunięcia, przekazany Zamawiającemu i ASI, oraz jeden skan kontrolny po usunięciu podatności krytycznych, nie później niż w terminie wykonania części.
4.6. Terminy wewnętrzne. Platforma wirtualizacji i maszyny wirtualne (pkt 4.2) do 11 grudnia 2026 r., skaner podatności i system monitoringu uruchomione (bez skanu kontrolnego i pełnej dokumentacji) do 15 grudnia 2026 r., całość części do 18 grudnia 2026 r. W przypadku udostępnienia serwera S13 później niż 8 grudnia 2026 r. terminy mogą zostać przedłużone aneksem o liczbę dni opóźnienia, nie dalej jednak niż do 23 grudnia 2026 r., na zasadach określonych w umowie; Wykonawca nie ponosi odpowiedzialności za opóźnienie z tej przyczyny.
4.7. Testy odbiorowe: utworzenie i uruchomienie maszyny testowej na magazynie macierzy; symulowana awaria jednego dysku, jeżeli konfiguracja na to pozwala; wykonanie kopii maszyny i odtworzenie jej z serwera S14 oraz z NAS przy odłączonym serwerze S14; wywołanie alertu w systemie monitoringu (odłączenie monitorowanego urządzenia) i potwierdzenie powiadomienia; uruchomienie skanu testowego i przegląd raportu; sprawdzenie dostępu administracyjnego wyłącznie z sieci zarządzania.

4.2.6.) Główny kod CPV: 72000000-5 - Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

4.2.7.) Dodatkowy kod CPV:

72263000-6 - Usługi wdrażania oprogramowania

72250000-2 - Usługi w zakresie konserwacji i wsparcia systemów

72220000-3 - Usługi doradcze w zakresie systemów i doradztwo techniczne

72800000-8 - Usługi audytu komputerowego i testowania komputerów

72600000-6 - Usługi doradcze i dodatkowe w zakresie sprzętu komputerowego

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: do 2026-12-18

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert:

4.3.1.) Sposób oceny ofert: Zamawiający wybiera najkorzystniejszą ofertę na podstawie kryteriów oceny ofert. Oferta złożona przez Wykonawcę może otrzymać łącznie 100 pkt.

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Punktowo

4.3.3.) Stosowane kryteria oceny ofert: Kryterium ceny oraz kryteria jakościowe

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 60

Kryterium 2

4.3.4.) Rodzaj kryterium: serwis posprzedażny, pomoc techniczna, warunki dostawy takich jak termin, sposób lub czas dostawy, oraz okresu realizacji.

4.3.5.) Nazwa kryterium: „Okres Wsparcia Po Odbiorze”

4.3.6.) Waga: 40

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

Część 3

4.2.2.) Krótki opis przedmiotu zamówienia

CZĘŚĆ 3 - SYSTEM INWENTARYZACJI I ZGŁOSZEŃ ORAZ INWENTARYZACJA AKTYWÓW IT
5.1. Przedmiot. Wdrożenie systemu GLPI (lub równoważnego) jako centralnej bazy aktywów (CMDB) i systemu obsługi zgłoszeń oraz wykonanie inwentaryzacji aktywów teleinformatycznych Zamawiającego z dokumentacją.
5.2. System GLPI:
1) instalacja na maszynie wirtualnej udostępnionej przez Zamawiającego (Część 2) albo, do czasu jej udostępnienia, w środowisku tymczasowym z późniejszym przeniesieniem; uwierzytelnianie użytkowników z Active Directory (LDAP), role: administrator, technik, użytkownik;
2) automatyczna inwentaryzacja: agent na wszystkich stacjach roboczych i serwerach, wykrywanie urządzeń sieciowych przez SNMP, powiązanie z użytkownikami i lokalizacjami (siedziba, obiekty technologiczne);
3) moduł zgłoszeń: kategorie, kolejki, priorytety i czasy obsługi uzgodnione z Zamawiającym, zgłaszanie przez interfejs i pocztą elektroniczną, powiadomienia, baza wiedzy z procedurami SZBI wskazanymi przez Zamawiającego, szablony dla wniosków o dostęp i zgłoszeń incydentów;
4) rejestr licencji i umów z dostawcami z terminami wygaśnięcia i powiadomieniami, rejestr cyklu życia sprzętu (wydanie, zwrot, wycofanie).
5.3. Inwentaryzacja aktywów IT:
1) spis z natury w siedzibie i na obiektach technologicznych (w części sieciowej IT i punktach styku z OT, bez ingerencji w sterowniki): sprzęt komputerowy, serwery, urządzenia sieciowe, urządzenia peryferyjne, nośniki, telefony służbowe, oprogramowanie i licencje, usługi zewnętrzne (hosting, poczta, systemy dziedzinowe), łącza;
2) dla każdego aktywa: identyfikator, typ, producent i model, numer seryjny, lokalizacja, użytkownik lub opiekun, właściciel aktywa, klasyfikacja informacji przetwarzanych według zasad SZBI Zamawiającego, status, data zakupu i koniec wsparcia, jeżeli są dostępne;
3) schemat logiczny sieci IT z adresacją i VLAN-ami, wykaz systemów i ich zależności, wykaz kont uprzywilejowanych i dostępów zewnętrznych (na podstawie informacji od ASI);
4) wynik inwentaryzacji wprowadzony do GLPI oraz przekazany w arkuszu w układzie rejestru aktywów Zamawiającego (wzór przekazuje Zamawiający) wraz z listą rozbieżności wobec dotychczasowej ewidencji i zaleceniami.
5.4. Testy odbiorowe: logowanie użytkownika domenowego i rejestracja zgłoszenia testowego z pełnym obiegiem;

sprawdzenie, że wszystkie stacje i serwery są widoczne w inwentarzu automatycznym; porównanie wybranych losowo 10 pozycji rejestru ze stanem faktycznym; przegląd schematu sieci.

4.2.6.) Główny kod CPV: 72000000-5 - Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

4.2.7.) Dodatkowy kod CPV:

72263000-6 - Usługi wdrażania oprogramowania

72250000-2 - Usługi w zakresie konserwacji i wsparcia systemów

72220000-3 - Usługi doradcze w zakresie systemów i doradztwo techniczne

72800000-8 - Usługi audytu komputerowego i testowania komputerów

72600000-6 - Usługi doradcze i dodatkowe w zakresie sprzętu komputerowego

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: do 2026-12-18

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert:

4.3.1.) Sposób oceny ofert: Zamawiający wybiera najkorzystniejszą ofertę na podstawie kryteriów oceny ofert. Oferta złożona przez Wykonawcę może otrzymać łącznie 100 pkt.

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Punktowo

4.3.3.) Stosowane kryteria oceny ofert: Kryterium ceny oraz kryteria jakościowe

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 60

Kryterium 2

4.3.4.) Rodzaj kryterium: serwis posprzedażny, pomoc techniczna, warunki dostawy takich jak termin, sposób lub czas dostawy, oraz okresu realizacji.

4.3.5.) Nazwa kryterium: „Okres Wsparcia Po Odbiorze”

4.3.6.) Waga: 40

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

Część 4

4.2.2.) Krótki opis przedmiotu zamówienia

CZĘŚĆ 4 - PROJEKT ARCHITEKTURY BEZPIECZEŃSTWA IT I NADZÓR NAD WDROŻENIEM
6.1. Przedmiot. Opracowanie projektu architektury bezpieczeństwa IT Zamawiającego oraz nadzór nad wdrożeniami realizowanymi w Częściach 1-3 i nad konfiguracją sieci wykonywaną przy dostawie przełączników.
6.2. Projekt architektury bezpieczeństwa IT, przekazany w terminie 7 dni roboczych od zawarcia umowy (wytyczne wstępne w terminie 3 dni roboczych, zgodnie z pkt 2.9), uzgodniony z Zamawiającym i ASI, obejmuje:
1) opis stanu obecnego na podstawie dokumentacji, wizji lokalnej i wywiadów (1 dzień w siedzibie);
2) architekturę docelową: segmentację sieci (strefy: użytkownicy, serwery, zarządzanie, kopie zapasowe, systemy bezpieczeństwa, goście, styk z siecią OT) z adresacją i VLAN-ami dla przełączników Cisco Catalyst 9200L, zasady ruchu między strefami dla zapory Stormshield, kontrolę dostępu 802.1X, szyfrowanie łącza między przełącznikami, dostęp administracyjny wyłącznie przez stację przesiadkową z uwierzytelnianiem kluczami FIDO2, kopie zapasowe w modelu 3-2-1, centralne zbieranie logów do SIEM, monitoring, zarządzanie podatnościami;
3) wytyczne konfiguracyjne dla wykonawców Części 1-3 i dla dostawcy przełączników (parametry, nazewnictwo, adresacja, integracje), listy kontrolne odbioru dla każdego wdrożenia;
4) odniesienie rozwiązań do wymagań ustawy o krajowym systemie cyberbezpieczeństwa, rozporządzenia KRI i normy ISO/IEC 27001 oraz do dokumentacji SZBI Zamawiającego, wraz z listą ryzyk pozostających po wdrożeniu i zaleceniami na

kolejne lata.
6.3. Nadzór nad wdrożeniem, do zakończenia ostatniego odbioru Części 1-3, nie później niż do 22 grudnia 2026 r.:
1) udział w uzgodnieniach i w odbiorach Części 1-3 oraz w odbiorze konfiguracji przełączników, weryfikacja zgodności z projektem i SOPZ według list kontrolnych, protokoły z uwagami;
2) bieżące konsultacje dla Zamawiającego i wykonawców (zdalnie, czas reakcji do końca następnego dnia roboczego), co najmniej dwie wizyty w siedzibie w okresie wdrożeń;
3) raport końcowy z nadzoru: stan wdrożeń, odstępstwa od projektu i ich uzasadnienie, otwarte zalecenia, ocena gotowości do eksploatacji, zaktualizowany schemat architektury powykonawczej;
4) niezależność nadzoru: jeżeli wykonawca Części 4 jest jednocześnie wykonawcą Części 1, 2 lub 3, zgodność tych wdrożeń z projektem i SOPZ potwierdza przy odbiorze wyłącznie Zamawiający z udziałem administratora systemów informatycznych, na podstawie list kontrolnych przygotowanych w ramach Części 4; wykonawca Części 4 nie potwierdza zgodności własnych prac, a w raporcie końcowym z nadzoru wyodrębnia te wdrożenia z opisem sposobu ich weryfikacji przez Zamawiającego. Nie zmienia to zakresu ani wynagrodzenia Części 4.
6.4. Testy odbiorowe: przyjęcie projektu przez Zamawiającego po uzgodnieniach; przyjęcie raportu końcowego z nadzoru wraz z kompletem list kontrolnych i protokołów. Nadzór jest świadczony do zakończenia ostatniego odbioru Części 1-3, nie później niż do 22 grudnia 2026 r.; raport końcowy i zgłoszenie wykonania Części 4 składa się w dniu ostatniego odbioru objętego nadzorem, nie później niż 22 grudnia, a odbiór Części 4 odbywa się tego samego dnia albo następnego dnia roboczego, nie później niż 23 grudnia 2026 r. Protokół odbioru Części 4 potwierdza czynności nadzorcze faktycznie wykonane do dnia ostatniego odbioru.

4.2.6.) Główny kod CPV: 72000000-5 - Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

4.2.7.) Dodatkowy kod CPV:

72263000-6 - Usługi wdrażania oprogramowania

72250000-2 - Usługi w zakresie konserwacji i wsparcia systemów

72220000-3 - Usługi doradcze w zakresie systemów i doradztwo techniczne

72800000-8 - Usługi audytu komputerowego i testowania komputerów

72600000-6 - Usługi doradcze i dodatkowe w zakresie sprzętu komputerowego

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: do 2026-12-22

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert:

4.3.1.) Sposób oceny ofert: Zamawiający wybiera najkorzystniejszą ofertę na podstawie kryteriów oceny ofert. Oferta złożona przez Wykonawcę może otrzymać łącznie 100 pkt.

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Punktowo

4.3.3.) Stosowane kryteria oceny ofert: Kryterium ceny oraz kryteria jakościowe

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 60

Kryterium 2

4.3.4.) Rodzaj kryterium: serwis posprzedażny, pomoc techniczna, warunki dostawy takich jak termin, sposób lub czas dostawy, oraz okresu realizacji.

4.3.5.) Nazwa kryterium: „Okres Wsparcia Po Odbiorze”

4.3.6.) Waga: 40

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

Część 5

4.2.2.) Krótki opis przedmiotu zamówienia

CZĘŚĆ 5 - TESTY BEZPIECZEŃSTWA INFRASTRUKTURY SIECIOWEJ
7.1. Przedmiot. Testy bezpieczeństwa infrastruktury sieciowej IT Zamawiającego metodą kontrolowanych testów penetracyjnych z weryfikacją ręczną, wykonane na podstawie pisemnego upoważnienia Zamawiającego określającego zakres adresów, okna czasowe i osoby do kontaktu, w terminie uzgodnionym z Zamawiającym między 7 a 18 grudnia 2026 r., tak aby objąć nowe przełączniki i systemy wdrożone w Częściach 1-3 w zakresie już uruchomionym. Przedmiotem testów jest przede wszystkim istniejąca infrastruktura (sieć biurowa, serwery, zapora, Active Directory, usługi dostępne z Internetu) oraz nowe przełączniki z segmentacją i kontrolą dostępu, które Zamawiający udostępnia do testów nie później niż 10 grudnia 2026 r.; platforma wirtualizacji i maszyny wirtualne są testowane w zakresie uruchomionym do dnia testów. System SIEM nie jest przedmiotem testów i jego wdrożenie (Część 1, termin 21 grudnia) nie warunkuje wykonania Części 5. Zamawiający zobowiązuje się udostępnić do testów istniejącą infrastrukturę oraz nowe przełączniki z segmentacją w uzgodnionym oknie między 7 a 18 grudnia; zakres określony w pkt 7.2 pkt 1-3 dla istniejącej infrastruktury stanowi pełny zakres pozycji U02 wniosku o dofinansowanie (skany, symulacje ataków, weryfikacja konfiguracji urządzeń, raport z rekomendacjami). Nowe elementy nieuruchomione do dnia testów nie są testowane, co nie zmniejsza zakresu usługi ani wynagrodzenia i nie wpływa na odbiór; Wykonawca wykazuje w raporcie, które elementy objęto testami, a które nie i z jakiej przyczyny, a Zamawiający potwierdza to w protokole odbioru. Wykonawca Części 5 nie odpowiada za opóźnienia innych wykonawców; retest w okresie wsparcia dotyczy wyłącznie elementów testowanych.
7.2. Zakres:
1) testy zewnętrzne: wszystkie adresy publiczne Zamawiającego (do 5 adresów) i usługi dostępne z Internetu, w tym dostęp zdalny i VPN;
2) testy wewnętrzne: sieć biurowa, serwery, urządzenia sieciowe, platforma wirtualizacji, stacja przesiadkowa (do 60 adresów), z pozycji użytkownika bez uprawnień i z pozycji urządzenia podłączonego do portu dostępowego, w tym próba obejścia kontroli dostępu 802.1X i segmentacji VLAN; sieć bezprzewodowa, jeżeli występuje;
3) przegląd konfiguracji Active Directory: polityka haseł, konta uprzywilejowane, delegacje, konta nieużywane, podatności typowe dla domeny; przegląd konfiguracji zapory sieciowej i przełączników pod kątem reguł i usług zbędnych;
4) testy wykonuje się bez technik odmowy usługi i bez ingerencji w sieć OT; próby eksploatacji podatności w systemach produkcyjnych wymagają zgody Zamawiającego; o podatnościach krytycznych Wykonawca informuje niezwłocznie, nie czekając na raport;
5) raport: streszczenie dla kierownictwa, wykaz podatności z oceną ważności (CVSS), opisem, dowodem i zaleceniem usunięcia, ocena skuteczności segmentacji i kontroli dostępu, lista zaleceń priorytetowych; omówienie raportu z Zamawiającym i ASI (do 2 godzin);
6) retest podatności krytycznych i wysokich po ich usunięciu, zgłoszony przez Zamawiającego w okresie wsparcia, z krótkim raportem.
7.3. Testy odbiorowe: przyjęcie raportu po omówieniu; raport zawiera wszystkie elementy z pkt 7.2 pkt 5.

4.2.6.) Główny kod CPV: 72000000-5 - Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

4.2.7.) Dodatkowy kod CPV:

72263000-6 - Usługi wdrażania oprogramowania

72250000-2 - Usługi w zakresie konserwacji i wsparcia systemów

72220000-3 - Usługi doradcze w zakresie systemów i doradztwo techniczne

72800000-8 - Usługi audytu komputerowego i testowania komputerów

72600000-6 - Usługi doradcze i dodatkowe w zakresie sprzętu komputerowego

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: do 2026-12-18

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert:

4.3.1.) Sposób oceny ofert: Zamawiający wybiera najkorzystniejszą ofertę na podstawie kryteriów oceny ofert. Oferta złożona przez Wykonawcę może otrzymać łącznie 100 pkt.

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Punktowo

4.3.3.) Stosowane kryteria oceny ofert: Kryterium ceny oraz kryteria jakościowe

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 60

Kryterium 2

4.3.4.) Rodzaj kryterium: serwis posprzedażny, pomoc techniczna, warunki dostawy takich jak termin, sposób lub czas dostawy, oraz okresu realizacji.

4.3.5.) Nazwa kryterium: „Okres Wsparcia Po Odbiorze”

4.3.6.) Waga: 40

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

Część 6

4.2.2.) Krótki opis przedmiotu zamówienia

CZĘŚĆ 6 - USŁUGA REAGOWANIA NA INCYDENTY
8.1. Przedmiot. Zapewnienie gotowości do reagowania na incydenty bezpieczeństwa w systemach IT Zamawiającego od dnia zawarcia umowy do końca dnia 18 grudnia 2026 r. wraz z pakietem 40 godzin prac specjalistów oraz ćwiczeniem reagowania. Zamawiający może zlecić przedłużenie gotowości na kolejne okresy w odrębnym zamówieniu.
8.2. Zakres:
1) przyjmowanie zgłoszeń telefonicznie i pocztą elektroniczną w dni robocze w godzinach 7:00-17:00 oraz telefonicznie w pozostałym czasie dla incydentów krytycznych (niedostępność systemów, podejrzenie oprogramowania szyfrującego, wyciek danych), z przystąpieniem do obsługi w czasie zadeklarowanym w ofercie (nie dłuższym niż 24 godziny od zgłoszenia, punktowane 4 i 8 godzin). Przystąpienie do obsługi oznacza potwierdzenie przyjęcia zgłoszenia i rozpoczęcie analizy przez specjalistę Wykonawcy, udokumentowane wiadomością do Zamawiającego; czas liczy się od zgłoszenia w godzinach przyjmowania zgłoszeń, a dla zgłoszeń poza tymi godzinami od godziny 7:00 następnego dnia roboczego, z wyjątkiem incydentów krytycznych zgłoszonych telefonicznie, dla których czas liczy się od zgłoszenia;
2) obsługa incydentu: analiza zdarzeń (w tym w SIEM po jego wdrożeniu), ustalenie zakresu i przyczyny, zalecenia powstrzymania i usunięcia skutków, wsparcie ASI w ich wykonaniu, zabezpieczenie dowodów, przygotowanie informacji do zgłoszenia incydentu poważnego do CSIRT NASK oraz naruszenia ochrony danych osobowych, raport z incydentu w terminie 5 dni roboczych od zakończenia obsługi; obsługa incydentu zgłoszonego w okresie gotowości jest kontynuowana po jego upływie do zakończenia w ramach pozostałych godzin pakietu, nie dłużej niż do 22 grudnia 2026 r., a jeżeli do tego dnia nie zostanie zakończona, Wykonawca przekazuje sprawę Zamawiającemu z dokumentacją dotychczasowych działań i zaleceniami, co kończy obsługę po stronie Wykonawcy; nowych incydentów po zakończeniu okresu gotowości nie przyjmuje się;
3) w ramach pakietu godzin, poza obsługą incydentów: ćwiczenie reagowania na incydent dla Kierownika, Pełnomocnika ds. SZBI i ASI (scenariusz ataku szyfrującego na infrastrukturę wodociągową, 4 godziny, w siedzibie lub zdalnie) z raportem i zaleceniami do procedury zarządzania incydentami Zamawiającego, oraz przegląd i dostosowanie progów alertów SIEM do procedury obsługi incydentów (do 4 godzin), wykonywane po udostępnieniu przez Zamawiającego działającego środowiska SIEM w zakresie umożliwiającym wykonanie czynności, bez konieczności wcześniejszego formalnego odbioru Części 1, w uzgodnieniu z wykonawcą Części 1 i udokumentowane notatką z wykazem zmienionych progów; czynności z niniejszego punktu są sposobem wykorzystania godzin pakietu, nie odrębnie wycenionym świadczeniem; jeżeli Zamawiający nie udostępni środowiska SIEM do 15 grudnia 2026 r., przegląd progów nie jest wykonywany, godziny pozostają do dyspozycji Zamawiającego na inne czynności z pkt 2 i 3 do 18 grudnia, ryczałt za gotowość i pakiet nie ulega zmianie, a Wykonawca nie odpowiada za opóźnienia wykonawcy Części 1;
4) ewidencja wykorzystanych godzin przekazywana Zamawiającemu po każdym zdarzeniu i zbiorczo na koniec umowy; godziny prac na miejscu liczone od przybycia do siedziby; dojazd w cenie usługi;
5) wynagrodzenie ryczałtowe obejmuje gotowość w całym okresie oraz pakiet 40 godzin niezależnie od liczby wykorzystanych godzin; godziny ponad pakiet mogą być zlecone odrębnie.
8.3. Testy odbiorowe: przeprowadzenie ćwiczenia i przyjęcie raportu z ćwiczenia; przyjęcie ewidencji godzin i raportów z incydentów, jeżeli wystąpiły; zawiadomienie o planowanym odbiorze do 16 grudnia; gotowość kończy się z upływem dnia 18 grudnia 2026 r.; zgłoszenie wykonania wraz z ewidencją gotowości (rejestr przyjętych zgłoszeń z datą i godziną, czasem przystąpienia i osobą), ewidencją wykorzystanych godzin, raportem z ćwiczenia oraz raportami z incydentów, dla których upłynął termin ich sporządzenia, składa się 21 grudnia 2026 r., a odbiór odbywa się 21 grudnia albo następnego dnia roboczego. W przypadku incydentów, których obsługa nie została zakończona lub dla których termin sporządzenia raportu jeszcze nie upłynął, Wykonawca przekazuje przy zgłoszeniu dokumentację dotychczasowych działań, a raport końcowy z obsługi takiego incydentu w terminie określonym w pkt 8.2 pkt 2, liczonym od zakończenia obsługi albo przekazania sprawy Zamawiającemu; przekazanie raportu potwierdza się pocztą elektroniczną, bez odrębnego protokołu. Odbiór Części 6 nie zwalnia Wykonawcy z obowiązku przekazania tego raportu. Zgłoszenia poza godzinami przyjmowania przyjęte 18 grudnia obsługuje się do zakończenia obsługi, co nie wydłuża okresu gotowości.

4.2.6.) Główny kod CPV: 72000000-5 - Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

4.2.7.) Dodatkowy kod CPV:

72263000-6 - Usługi wdrażania oprogramowania

72250000-2 - Usługi w zakresie konserwacji i wsparcia systemów

72220000-3 - Usługi doradcze w zakresie systemów i doradztwo techniczne

72800000-8 - Usługi audytu komputerowego i testowania komputerów

72600000-6 - Usługi doradcze i dodatkowe w zakresie sprzętu komputerowego

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: do 2026-12-18

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert:

4.3.1.) Sposób oceny ofert: Zamawiający wybiera najkorzystniejszą ofertę na podstawie kryteriów oceny ofert. Oferta złożona przez Wykonawcę może otrzymać łącznie 100 pkt.

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Punktowo

4.3.3.) Stosowane kryteria oceny ofert: Kryterium ceny oraz kryteria jakościowe

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 60

Kryterium 2

4.3.4.) Rodzaj kryterium: serwis posprzedażny, pomoc techniczna, warunki dostawy takich jak termin, sposób lub czas dostawy, oraz okresu realizacji.

4.3.5.) Nazwa kryterium: „Czas przystąpienia do obsługi incydentu”

4.3.6.) Waga: 40

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

SEKCJA V - KWALIFIKACJA WYKONAWCÓW

5.1.) Zamawiający przewiduje fakultatywne podstawy wykluczenia: Nie

5.3.) Warunki udziału w postępowaniu: Tak

5.4.) Nazwa i opis warunków udziału w postępowaniu.
CZĘŚĆ 1 – Wdrożenie systemu klasy SIEM

Wykonawca musi wykazać, że:

Posiada odpowiednie doświadczenie, tj. w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, należycie wykonał co najmniej jedną usługę wdrożenia systemu klasy SIEM obejmującą co najmniej 20 źródeł zdarzeń (agentów lub urządzeń).

Dysponuje odpowiednim personelem, tj. skieruje do realizacji zamówienia co najmniej jedną osobę, która uczestniczyła w co najmniej jednym wdrożeniu systemu klasy SIEM.

CZĘŚĆ 2 – Wdrożenie platformy wirtualizacji i systemów monitoringu lub skanowania podatności

Wykonawca musi wykazać, że:

1. Posiada odpowiednie doświadczenie, tj. w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, należycie wykonał:

co najmniej jedną usługę wdrożenia platformy wirtualizacji serwerów; co najmniej jedną usługę wdrożenia systemu monitoringu infrastruktury lub skanera podatności.

Wskazane usługi mogą wynikać z jednej umowy.
2. Dysponuje odpowiednim personelem, tj. skieruje do realizacji zamówienia co najmniej jedną osobę posiadającą doświadczenie w administrowaniu platformą wirtualizacji i systemami Linux.

CZĘŚĆ 3 – Wdrożenie systemu inwentaryzacji lub obsługi zgłoszeń (ITSM)

Wykonawca musi wykazać, że:
Posiada odpowiednie doświadczenie, tj. w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, należycie wykonał co najmniej jedną usługę: wdrożenia systemu inwentaryzacji lub obsługi zgłoszeń (ITSM), lub inwentaryzacji aktywów teleinformatycznych, dla podmiotu posiadającego co najmniej 15 stanowisk.
2. Dysponuje odpowiednim personelem, tj. skieruje do realizacji zamówienia co najmniej jedną osobę, która wykonywała inwentaryzację aktywów lub uczestniczyła we wdrożeniu systemu ITSM.

CZĘŚĆ 4 – Opracowanie projektu lub koncepcji architektury bezpieczeństwa IT albo audyt bezpieczeństwa

Wykonawca musi wykazać, że: Posiada odpowiednie doświadczenie, tj. w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, należycie wykonał co najmniej jedną usługę: opracowania projektu lub koncepcji architektury bezpieczeństwa IT, lub przeprowadzenia audytu bezpieczeństwa infrastruktury teleinformatycznej.

Dysponuje odpowiednim personelem, tj. skieruje do realizacji zamówienia co najmniej jedną osobę: posiadającą certyfikat CISSP, CISA, CISM, audytora wiodącego ISO/IEC 27001 lub równoważny, lub posiadającą co najmniej 3-letnie doświadczenie w projektowaniu lub audytowaniu bezpieczeństwa infrastruktury IT.

CZĘŚĆ 5 – Testy penetracyjne infrastruktury sieciowej

Wykonawca musi wykazać, że: Posiada odpowiednie doświadczenie, tj. w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, należycie wykonał co najmniej dwie usługi testów penetracyjnych infrastruktury sieciowej, zakończone sporządzeniem raportów.

Dysponuje odpowiednim personelem, tj. skieruje do realizacji zamówienia co najmniej jedną osobę: posiadającą certyfikat OSCP, eCPPT, CEH Practical, OSCE lub równoważny, lub posiadającą udokumentowany udział w co najmniej trzech testach penetracyjnych infrastruktury.

CZĘŚĆ 6 – Obsługa lub reagowanie na incydenty bezpieczeństwa

Wykonawca musi wykazać, że: Posiada odpowiednie doświadczenie, tj. w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, należycie wykonał co najmniej jedną usługę obsługi lub reagowania na incydenty bezpieczeństwa, w tym usługę typu SOC lub gotowości do reagowania, świadczoną przez okres co najmniej 3 miesięcy.

Dysponuje odpowiednim personelem, tj. skieruje do realizacji zamówienia co najmniej jedną osobę posiadającą co najmniej 2-letnie doświadczenie w obsłudze incydentów bezpieczeństwa.

Uwaga: Warunki dotyczące doświadczenia wykonawcy oraz kwalifikacji i doświadczenia osób skierowanych do realizacji zamówienia należy wykazać odrębnie dla każdej części zamówienia, na którą wykonawca składa ofertę.

5.5.) Zamawiający wymaga złożenia oświadczenia, o którym mowa w art.125 ust. 1 ustawy: Tak

5.6.) Wykaz podmiotowych środków dowodowych na potwierdzenie niepodlegania wykluczeniu: Oświadczenia wykonawcy o aktualności informacji zawartych w oświadczeniu o którym mowa w art. 125 ust. 1 ustawy Pzp, w
zakresie podstaw wykluczenia z
postępowania wskazanych przez zamawiającego (załącznik nr 11 do SWZ), o których mowa w:
a) art. 108 ust. 1 ustawy PZP
b) w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022r. poz. 835 o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

5.7.) Wykaz podmiotowych środków dowodowych na potwierdzenie spełniania warunków udziału w postępowaniu:
Podmiotowe środki dowodowe (aktualne na dzień ich złożenia) składane na wezwanie Zamawiającego, zgodnie z art. 274 ust. 1 Pzp - składa wykonawca, którego oferta została najwyżej oceniona, w wyznaczonym terminie, nie krótszym niż 5 dni:
1) wykaz osób (załącznik nr 8 do SWZ) - DOTYCZY CZĘŚCI OD 1 DO 6
wykaz osób o kwalifikacjach wskazanych w pkt. 6 ppkt 1 d) niniejszego rozdziału, według wzoru stanowiących załącznik do SWZ.
Dokumenty składa się w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub osobistym, zgodnie z rozporządzeniem w sprawie podmiotowych środków dowodowych.

2) wykaz usług (załącznik nr 8A do SWZ) - DOTYCZY CZĘŚCI OD 1 DO 6
wykaz usług, w okresie ostatnich 3 lat przed upływem terminu składania ofert (a jeżeli okres prowadzenia działalności jest krótszy, w tym okresie) należycie wykonał usługi wskazane w pkt. 6 ppkt 1 d) niniejszego rozdziału wraz z dowodami należytego wykonania. Dokumenty składa się w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub osobistym, zgodnie z rozporządzeniem w sprawie podmiotowych środków dowodowych.

SEKCJA VI - WARUNKI ZAMÓWIENIA

6.1.) Zamawiający wymaga albo dopuszcza oferty wariantowe: Nie

6.3.) Zamawiający przewiduje aukcję elektroniczną: Nie

6.4.) Zamawiający wymaga wadium: Nie

6.5.) Zamawiający wymaga zabezpieczenia należytego wykonania umowy: Nie

6.6.) Wymagania dotyczące składania oferty przez wykonawców wspólnie ubiegających się o udzielenie zamówienia:
Wymagania dotyczące składania oferty przez wykonawców wspólnie ubiegających się o udzielenie zamówienia:
1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia (w tym spółki cywilne, konsorcja).
2. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia zobligowani są do ustanowienia Pełnomocnika do reprezentowania ich w niniejszym postępowaniu albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo winno być załączone do oferty.
3. Wykonawcy ponoszą solidarną odpowiedzialność za wykonanie umowy.
4. Wszelka korespondencja prowadzona będzie wyłącznie z Pełnomocnikiem wykonawców.
5. Przepisy dotyczące Wykonawcy stosuje się odpowiednio do wykonawców wspólnie ubiegających się o udzielenie zamówienia.
6. W odniesieniu do Wykonawców wspólnie ubiegających się o udzielenie zamówienia Zamawiający nie określa wymagań związanych z realizacją zamówienia w inny sposób niż w odniesieniu do pojedynczych wykonawców.
7. Oferta musi być podpisana w sposób, który prawnie zobowiązuje wszystkich Wykonawców występujących wspólnie.
8. Zgodnie z art. 117 ust. 4 PZP w przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia, wykonawcy dołączają do oferty oświadczenie, z którego wynika, które roboty budowlane, dostawy lub usługi wykonują poszczególni wykonawcy.

6.7.) Zamawiający przewiduje unieważnienie postępowania, jeśli środki publiczne, które zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia nie zostały przyznane: Tak

SEKCJA VII - PROJEKTOWANE POSTANOWIENIA UMOWY

7.1.) Zamawiający przewiduje udzielenia zaliczek: Nie

7.3.) Zamawiający przewiduje zmiany umowy: Tak

7.4.) Rodzaj i zakres zmian umowy oraz warunki ich wprowadzenia:
Zakres dopuszczalnych zmian umowy określa paragraf 10 projektu umowy (załącznik nr 4 do SWZ)

7.5.) Zamawiający uwzględnił aspekty społeczne, środowiskowe, innowacyjne lub etykiety związane z realizacją zamówienia: Nie

SEKCJA VIII – PROCEDURA

8.1.) Termin składania ofert: 2026-11-18 08:00

8.2.) Miejsce składania ofert: https://niechlow.ezamawiajacy.pl/pn/niechlow/demand/336134/notice/public/details

8.3.) Termin otwarcia ofert: 2026-11-18 08:30

8.4.) Termin związania ofertą: 30 dni