515394-2026 - Súťaž

Poľsko – Počítačové zariadenia a spotrebný materiál – Zwiększenie cyberodporności i ciągłości działania Przedsiębiorstwa Komunalnego Sp. z o.o. w Siemiatyczach. Część II - Obszar kompetencyjny oraz obszar techniczny IT.
OJ S 141/2026 24/07/2026
Oznámenie o vyhlásení verejného obstarávania alebo oznámenie o koncesii – štandardný režim - Oznámenie o zmene
Tovary - Služby

1. Kupujúci

1.1. Kupujúci

Úradný názov: PRZEDSIĘBIORSTWO KOMUNALNE SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
E-mail: sekretariat@pksiemiatycze.pl
Typ kupujúceho podľa právnych predpisov: Verejnoprávna inštitúcia pod kontrolou miestneho orgánu
Činnosť verejného obstarávateľa: Všeobecné verejné služby

2. Postup

2.1. Postup

Názov: Zwiększenie cyberodporności i ciągłości działania Przedsiębiorstwa Komunalnego Sp. z o.o. w Siemiatyczach. Część II - Obszar kompetencyjny oraz obszar techniczny IT.
Opis: 1. Przedmiot zamówienia jest finansowany ze środków Programu Krajowy Plan Odbudowy i Zwiększania Odporności, Priorytet: C3 Cyberbezpieczeństwo. Działanie: C3.1.1. Cyberbezpieczeństwo – CyberPL. 2. Projekt ma na celu wzmocnienie cyberodporności poprzez modernizację infrastruktury oraz rozwój kompetencji zespołów. W ramach projektu zrealizowane zostaną działania: 1) Modernizacja infrastruktury sieciowej: Wdrożenie segmentacji i mikrosegmentacji sieci IT/OT, co umożliwi izolację newralgicznych systemów i minimalizację potencjalnych szkód w przypadku ataku. Zostanie również wdrożony system monitorowania ruchu sieciowego (IDS/IPS). Umożliwi on gromadzenie logów systemowych i dowodów cyfrowych niezbędnych do analizy incydentów. 2) Wdrożenie bezpiecznych zdalnych dostępów: Wprowadzenie scentralizowanego i bezpiecznego systemu zdalnego dostępu, który pozwoli na kontrolę i audytowanie połączeń z sieciami OT/IT. 3) Zapewnienie ciągłości działania: Zostanie wdrożony system do tworzenia i zarządzania kopiami zapasowymi, w tym również dla systemów sterowania, co zapewni szybki powrót do sprawności w przypadku incydentu. 3. Projekt jest zgodny z priorytetami KPO i Zwiększania Odporności, a w szczególności z celem Transformacji Cyfrowej. Inwestycja w nowoczesne technologie cyberbezpieczeństwa jest kluczowym elementem w dążeniu do stworzenia bezpiecznej infrastruktury krytycznej, zapewniającej ciągłość świadczenia usług publicznych. 4. Wdrożenie Części II projektu (Obszar kompetencyjny oraz obszar techniczny IT)polega na realizacji zadań: 1) Zadanie 1. Szkolenia z zakresu cyberbezpieczeństwa - szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach Projektu grantowego IT /OT/ICS. 2) Zadanie 2. Oprogramowanie do badania podatności. 3) Zadanie 3. Oprogramowanie do ochrony przed ransomware. 4) Zadanie 4. Oprogramowanie typu EDR (Endpoint Detection and Response). 5) Zadanie 5. Urządzenie i oprogramowanie typu NDR z

HoneyPot i monitorem sytuacyjnym (Network Detection & Response). 6) Zadanie 6. Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu open source IT/ICS/IIoT. 7) Zadanie 7. System typu UTM dla sieci IT HA Przedmiot zamówienia. 8) Zadanie 8. Usługi konfiguracji i hardeningu systemów/urządzeń IT. 9) Zadanie 9. Stacja robocza fizyczna z rolą stacji przesiadkowej (broker sesji) + dwa monitory 27 cali - 1 komplet. 10) Zadanie 10. Usługa segmentacji sieci . 11) Zadanie 11. Serwer do wykonywania kopii zapasowych (NAS). 12) Zadanie 12. Zarządzalny switch L2, 48p GE PoE + 4× SFP+ (2 szt.). 13) Zadanie 13. Zarządzalny switch L2, 16p GE + 2× SFP (6 szt.). 14) Zadanie 14. Access Point WiFi z obsługą standardu 802.1x oraz WPA3-Enterprise. 15) Zadanie 15. Oprogramowanie typu ITSM (Information Technology Service Management). 16) Zadanie 16. Oprogramowanie typu MDM (Mobile Device Management) Przedmiot zamówienia. 17) Zadanie 17. Oprogramowanie przeciwdziałającemu wyciekowi danych (DLP - Data Leak Prevention). 18) Zadanie 18. Usługa typu MDR (Managed Detection and Response) IT/OT/ICS/IIoT. 19) Zadanie 19. Oprogramowanie do zarządzania tożsamością i dostępem. 20) Zadanie 20. Oprogramowanie lub urządzenie typu MFA (dwu-/wieloskładnikowe uwierzytelnianie). 21) Zadanie 21. Klucze sprzętowe U2F. 22) Zadanie 22. Usługa inwentaryzacji aktywów teleinformatycznych OT/ICS/IIoT. 23) Zadanie 23. Dostawa sprzętowych sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych). 24) Zadanie 24. Dostawa sprzętowych sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych). 25) Zadanie 25. Oprogramowanie / licencje IDS (Intrusion Detection System) dedykowany sieciom OT. Oprogramowanie zintegrowany System bezpieczeństwa-Industrial Central Management dla OT, Anomaly Detection, Threat Detection, Data Traceability Control, Anti DDOS, APT (Advanced Persistent Threat), SIEM, SOAR, Active Dashboards, Central FW MGMT, Alarm Risk MGMT. 26) Zadanie 26. UTM (Unified Threat Management) Platforma sprzętowa DIN35 lub desktop - System bezpieczeństwa IPS/IDS, IT/OTAnomaly Detection, Threat Detection, Data Traceability Control, SDN, Anti DDOS, Anti APT (Advanced Persistent Threat), AI MGMT, ZBFW. 27) Zadanie 27. Usługa Private APN. 28) Zadanie 28. Usługa inwentaryzacji aktywów teleinformatycznych IT. 29) Zadanie 29. Zaprojektowanie rozwiązania z zakresu bezpieczeństwa z doborem urządzeń, oprogramowania i usług wdrożenia i eksploatacji IT/OT /ICS/IoT. 30) Zadanie 30. Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu open source IT/OT/ICS/IIo. 31) Zadanie 31. Testy bezpieczeństwa infrastruktury sieciowej IT/OT/ICS/IIoT. 32) Zadanie 32. Usługi konfiguracji i hardeningu systemów/urządzeń OT/ICS/IIoT. 5. Opis przedmiotu zamówienia wraz z określeniem minimalnych wymagań został przedstawiony w Załączniku nr 2 do SWZ – Szczegółowy Opis Przedmiotu Zamówienia (SOPZ).
Identifikátor postupu: 1ed3396f-1a0a-46ea-a0c4-ff893173fa76
Interný identifikátor: ZWiK.4500.2.5.2025
Druh postupu: Verejná súťaž
Postup je zrýchlený: nie

2.1.1. Účel

Druh zmluvy: Tovary
Doplňujúci druh zmluvy: Služby
Hlavná klasifikácia (cpv): 30200000 Počítačové zariadenia a spotrebný materiál
Doplňujúca klasifikácia (cpv): 32420000 Sieťové zariadenia, 32422000 Sieťové komponenty, 35100000 Pohotovostné a zabezpečovacie zariadenia, 35121000 Zabezpečovacie zariadenie, 48000000 Softvérové balíky a informačné systémy, 48210000 Softvérový balík na vytváranie sietí, 48600000 Databázový a operačný softvérový balík, 48730000 Softvérový balík na zaistenie bezpečnosti, 48732000 Softvérový balík na zaistenie bezpečnosti dát, 48820000

Servery, 48821000 Sieťové servery, 48900000 Rôzne softvérové balíky a počítačové systémy, 51611100 Inštalácia technického vybavenia (hardvér) počítačov, 72222000 Strategické prehodnotenie a plánovanie informačných systémov alebo technológie, 72263000 Implementácia softvéru, 72265000 Konfigurovanie softvéru, 72315000 Riadenie a podpora dátových sietí, 72600000 Počítačové podporné služby a poradenstvo, 73431000 Skúšanie a hodnotenie bezpečnostného vybavenia, 79212000 Audítorské služby, 79417000 Bezpečnostné poradenstvo, 80510000 Služby týkajúce sa odborných školení, 80533100 Školenia na prácu s počítačmi, 80550000 Bezpečnostné školenia

2.1.2. Miesto plnenia

Mesto: Siemiatycze
PSČ: 17-300
Nižšia územná jednotka krajiny (NUTS): Łomżyński (PL842)
Krajina: Poľsko

2.1.4. Všeobecné informácie

Právny základ:
Smernica 2014/24/EÚ

2.1.6. Dôvody na vylúčenie

Zdroje dôvodov na vylúčenie: Oznámenie
Priama alebo nepriama účasť na príprave tohto postupu obstarávania: Dotyczy art. 108 ust. 1 pkt 6 ustawy Pzp.
Korupcia: Dotyczy art. 108 ust. 1 pkt 1 i 2 ustawy Pzp.
Podvod: Dotyczy art. 108 ust. 1 pkt 1 i 2 ustawy Pzp.
Porušenie povinností v oblasti pracovného práva: Dotyczy art. 108 ust. 1 pkt 1 lit. h i pkt 2 ustawy Pzp.
Porušenie povinnosti platiť príspevky na sociálne zabezpečenie: Dotyczy art. 108 ust. 1 pkt 3 ustawy Pzp.
Porušenie povinnosti platiť dane: Dotyczy art. 108 ust. 1 pkt 3 ustawy Pzp.
Čisto vnútroštátne dôvody vylúčenia: Dotyczy art.108 ust. 1 pkt 1 ustawy Pzp. Dotyczy art.108 ust. 1 pkt 4 ustawy Pzp. Dotyczy art. 108 ust. 2 ustawy Pzp.
Dohody s inými hospodárskymi subjektmi s cieľom narušiť hospodársku súťaž: Dotyczy art. 108 ust. 1 pkt 5 ustawy Pzp.
Detská práca a iné formy obchodovania s ľuďmi: Dotyczy art. 108 ust. 1 pkt 1 i 2 ustawy Pzp.
Pranie špinavých peňazí alebo financovanie terorizmu: Dotyczy art. 108 ust. 1 pkt 1 i 2 ustawy Pzp.
Teroristické trestné činy alebo trestné činy spojené s teroristickými činnosťami: Dotyczy art. 108 ust. 1 pkt 1 i 2 ustawy Pzp.
Účasť v zločineckej organizácii: Dotyczy art. 108 ust. 1 pkt 1 i 2 ustawy Pzp.

5. Časť

5.1. Časť: LOT-0001

Názov: Zwiększenie cyberodporności i ciągłości działania Przedsiębiorstwa Komunalnego Sp. z o.o. w Siemiatyczach poprzez wdrożenie nowoczesnych rozwiązań, modernizację infrastruktury oraz podniesienie kompetencji personelu. Część II - Obszar kompetencyjny oraz obszar techniczny IT
Opis: 1. Przedmiot zamówienia jest finansowany ze środków Programu Krajowy Plan Odbudowy i Zwiększania Odporności, Priorytet: C3 Cyberbezpieczeństwo. Działanie: C3.1.1. Cyberbezpieczeństwo – CyberPL. 2. Projekt ma na celu wzmocnienie cyberodporności

poprzez modernizację infrastruktury oraz rozwój kompetencji zespołów. W ramach projektu zrealizowane zostaną działania: 1) Modernizacja infrastruktury sieciowej: Wdrożenie segmentacji i mikrosegmentacji sieci IT/OT, co umożliwi izolację newralgicznych systemów i minimalizację potencjalnych szkód w przypadku ataku. Zostanie również wdrożony system monitorowania ruchu sieciowego (IDS/IPS). Umożliwi on gromadzenie logów systemowych i dowodów cyfrowych niezbędnych do analizy incydentów. 2) Wdrożenie bezpiecznych zdalnych dostępów: Wprowadzenie scentralizowanego i bezpiecznego systemu zdalnego dostępu, który pozwoli na kontrolę i audytowanie połączeń z sieciami OT/IT. 3) Zapewnienie ciągłości działania: Zostanie wdrożony system do tworzenia i zarządzania kopiami zapasowymi, w tym również dla systemów sterowania, co zapewni szybki powrót do sprawności w przypadku incydentu. 3. Projekt jest zgodny z priorytetami KPO i Zwiększania Odporności, a w szczególności z celem Transformacji Cyfrowej. Inwestycja w nowoczesne technologie cyberbezpieczeństwa jest kluczowym elementem w dążeniu do stworzenia bezpiecznej infrastruktury krytycznej, zapewniającej ciągłość świadczenia usług publicznych. 4. Wdrożenie Części II projektu (Obszar kompetencyjny oraz obszar techniczny IT)polega na realizacji zadań: 1) Zadanie 1. Szkolenia z zakresu cyberbezpieczeństwa - szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa w ramach Projektu grantowego IT /OT/ICS. 2) Zadanie 2. Oprogramowanie do badania podatności. 3) Zadanie 3. Oprogramowanie do ochrony przed ransomware. 4) Zadanie 4. Oprogramowanie typu EDR (Endpoint Detection and Response). 5) Zadanie 5. Urządzenie i oprogramowanie typu NDR z HoneyPot i monitorem sytuacyjnym (Network Detection & Response). 6) Zadanie 6. Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu open source IT/ICS/IIoT. 7) Zadanie 7. System typu UTM dla sieci IT HA Przedmiot zamówienia. 8) Zadanie 8. Usługi konfiguracji i hardeningu systemów/urządzeń IT. 9) Zadanie 9. Stacja robocza fizyczna z rolą stacji przesiadkowej (broker sesji) + dwa monitory 27 cali - 1 komplet. 10) Zadanie 10. Usługa segmentacji sieci . 11) Zadanie 11. Serwer do wykonywania kopii zapasowych (NAS). 12) Zadanie 12. Zarządzalny switch L2, 48p GE PoE + 4× SFP+ (2 szt.). 13) Zadanie 13. Zarządzalny switch L2, 16p GE + 2× SFP (6 szt.). 14) Zadanie 14. Access Point WiFi z obsługą standardu 802.1x oraz WPA3-Enterprise. 15) Zadanie 15. Oprogramowanie typu ITSM (Information Technology Service Management). 16) Zadanie 16. Oprogramowanie typu MDM (Mobile Device Management) Przedmiot zamówienia. 17) Zadanie 17. Oprogramowanie przeciwdziałającemu wyciekowi danych (DLP - Data Leak Prevention). 18) Zadanie 18. Usługa typu MDR (Managed Detection and Response) IT/OT/ICS/IIoT. 19) Zadanie 19. Oprogramowanie do zarządzania tożsamością i dostępem. 20) Zadanie 20. Oprogramowanie lub urządzenie typu MFA (dwu-/wieloskładnikowe uwierzytelnianie). 21) Zadanie 21. Klucze sprzętowe U2F. 22) Zadanie 22. Usługa inwentaryzacji aktywów teleinformatycznych OT/ICS/IIoT. 23) Zadanie 23. Dostawa sprzętowych sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych). 24) Zadanie 24. Dostawa sprzętowych sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych). 25) Zadanie 25. Oprogramowanie / licencje IDS (Intrusion Detection System) dedykowany sieciom OT. Oprogramowanie zintegrowany System bezpieczeństwa-Industrial Central Management dla OT, Anomaly Detection, Threat Detection, Data Traceability Control, Anti DDOS, APT (Advanced Persistent Threat), SIEM, SOAR, Active Dashboards, Central FW MGMT, Alarm Risk MGMT. 26) Zadanie 26. UTM (Unified Threat Management) Platforma sprzętowa DIN35 lub desktop - System bezpieczeństwa IPS/IDS, IT/OTAnomaly Detection, Threat Detection, Data Traceability Control, SDN, Anti DDOS, Anti APT (Advanced Persistent Threat), AI MGMT, ZBFW. 27) Zadanie 27. Usługa Private APN. 28) Zadanie 28. Usługa inwentaryzacji aktywów teleinformatycznych IT. 29) Zadanie 29. Zaprojektowanie rozwiązania z zakresu

bezpieczeństwa z doborem urządzeń, oprogramowania i usług wdrożenia i eksploatacji IT/OT /ICS/IoT. 30) Zadanie 30. Wdrożenie urządzeń/oprogramowania/rozwiązania z zakresu bezpieczeństwa. Dotyczy to również rozwiązań typu open source IT/OT/ICS/IIo. 31) Zadanie 31. Testy bezpieczeństwa infrastruktury sieciowej IT/OT/ICS/IIoT. 32) Zadanie 32. Usługi konfiguracji i hardeningu systemów/urządzeń OT/ICS/IIoT. 5. Opis przedmiotu zamówienia wraz z określeniem minimalnych wymagań został przedstawiony w Załączniku nr 2 do SWZ – Szczegółowy Opis Przedmiotu Zamówienia (SOPZ).
Interný identifikátor: ZWiK.4500.2.5.2025

5.1.1. Účel

Druh zmluvy: Tovary
Doplňujúci druh zmluvy: Služby
Hlavná klasifikácia (cpv): 30200000 Počítačové zariadenia a spotrebný materiál
Doplňujúca klasifikácia (cpv): 32420000 Sieťové zariadenia, 32422000 Sieťové komponenty, 35100000 Pohotovostné a zabezpečovacie zariadenia, 35121000 Zabezpečovacie zariadenie, 48000000 Softvérové balíky a informačné systémy, 48210000 Softvérový balík na vytváranie sietí, 48600000 Databázový a operačný softvérový balík, 48730000 Softvérový balík na zaistenie bezpečnosti, 48732000 Softvérový balík na zaistenie bezpečnosti dát, 48820000 Servery, 48821000 Sieťové servery, 48900000 Rôzne softvérové balíky a počítačové systémy, 51611100 Inštalácia technického vybavenia (hardvér) počítačov, 72222000 Strategické prehodnotenie a plánovanie informačných systémov alebo technológie, 72263000 Implementácia softvéru, 72265000 Konfigurovanie softvéru, 72315000 Riadenie a podpora dátových sietí, 72600000 Počítačové podporné služby a poradenstvo, 73431000 Skúšanie a hodnotenie bezpečnostného vybavenia, 79212000 Audítorské služby, 79417000 Bezpečnostné poradenstvo, 80533100 Školenia na prácu s počítačmi, 80510000 Služby týkajúce sa odborných školení, 80550000 Bezpečnostné školenia

5.1.2. Miesto plnenia

Mesto: Siemiatycze
PSČ: 17-300
Nižšia územná jednotka krajiny (NUTS): Łomżyński (PL842)
Krajina: Poľsko

5.1.3. Predpokladané trvanie

Dátum začatia: 14/09/2026
Dátum konca trvania: 10/12/2026

5.1.6. Všeobecné informácie

Vyhradená účasť:
Účasť nie je vyhradená.
Je povinné uviesť mená a odbornú kvalifikáciu zamestnancov určených na plnenie zmluvy: Nevyžaduje sa
Projekt verejného obstarávania úplne alebo čiastočne financovaný z prostriedkov EÚ
Informácie o fondoch Európskej únie:
Identifikátor finančných prostriedkov EÚ: Program Krajowy Plan Odbudowy i Zwiększania Odporności.
Viac podrobností o finančných prostriedkoch EÚ: Priorytet: C3 Cyberbezpieczeństwo. Działanie: C3.1.1. Cyberbezpieczeństwo – CyberPL Konkurs grantowy pn. „Cyberbezpieczne Wodociągi” o numerze KPOD.05.10-CW.01-001/25 Tytuł projektu: Zwiększenie

cyberodporności i ciągłości działania Przedsiębiorstwa Komunalnego Sp. z o.o. w Siemiatyczach poprzez wdrożenie nowoczesnych rozwiązań, modernizację infrastruktury oraz podniesienie kompetencji personelu.
Na toto verejné obstarávanie sa vzťahuje Dohoda o vládnom obstarávaní (GPA): nie
Toto verejné obstarávanie je vhodné aj pre malé a stredné podniky (MSP): áno

5.1.9. Kritériá výberu

Zdroje výberových kritérií: Oznámenie
Kritérium: Poistenie profesijného rizika
Popis výberového kritéria: Wykonawca powinien wykazać, że posiada ubezpieczenie od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia (w szczególności ryzyk cybernetycznych) na sumę gwarancyjną nie mniejszą niż 300 000 zł (słownie: trzysta tysięcy złotych). Wykonawca obowiązany jest utrzymać ważność ubezpieczenia przez cały okres realizacji Umowy.

Kritérium: Relevantné vzdelávacie a profesionálne kvalifikácie
Popis výberového kritéria: Wykonawca powinien wskazać co najmniej dwie osoby zatrudnione przez Wykonawcę – specjalistów odpowiedzialnych za wdrożenia rozwiązań objętych niniejszym przedmiotem zamówienia, posiadających niezbędną wiedzę i doświadczenie potwierdzone co najmniej 4-letnim stażem pracy związanym z wdrożeniami systemów cyberbezpieczeństwa oraz wykształceniem wyższym na kierunku informatycznym, oraz z ważnymi certyfikatami oferowanych rozwiązań z cyberbezpieczeństwa IT oraz OT na poziomie Professional.

Kritérium: Referencie na špecifikované dodávky
Popis výberového kritéria: Wykonawca powinien wykazać, że w okresie ostatnich trzech lat przed dniem, w którym upływa termin składania ofert, a jeżeli okres prowadzenia działalności jest krótszy to w tym okresie, zrealizował co najmniej sześć dostaw lub usług, związanych z wdrażaniem systemów bezpieczeństwa, w ramach której zrealizowano co najmniej: - jedno (1) zamówienie na dostawę rozwiązań z zakresu cyberbezpieczeństwa, przy czym w skład rozwiązania wchodził minimum serwer, macierz dyskowa, systemy do backupu, o wartości zamówienia nie mniejszej niż 200 000,00 złotych brutto; - jedno (1) zamówienie na dostawę systemów bezpieczeństwa sieci, zapory sieciowe NGFW, IPS, NDR, o wartości zamówienia nie mniejszej niż 400 000,00 złotych brutto; - jedno (1) zamówienie na dostawę systemów bezpieczeństwa klasy SIEM, o wartości zamówienia nie mniejszej niż 500 000,00 złotych brutto;

Kritérium: Opatrenia na zabezpečenie kvality
Popis výberového kritéria: Wykonawca musi posiadać aktualną autoryzację lub partnerstwo techniczne wystawione przez producenta rozwiązania oferowanego w niniejszym postępowaniu, potwierdzające prawo do jego sprzedaży, wdrażania i świadczenia wsparcia technicznego na terytorium Rzeczypospolitej Polskiej. Wymóg ten stosuje się odpowiednio do każdego producenta; w przypadku oferty wieloproducentowej dopuszczany jest dowód równoważny (Multivendor).

5.1.10. Kritériá na vyhodnotenie ponúk

Kritérium:
Typ: Cena
Názov: Cena

Opis: 1. Ocena ofert będzie dokonywana według skali punktowej, przy założeniu, że maksymalna punktacja wynosi 100 punktów. 2. Zamawiający dokona oceny ofert przyznając punkty w ramach poszczególnych kryteriów oceny ofert, przyjmując zasadę, że 1% = 1 punkt. 3. Przy wyborze oferty Zamawiający będzie się kierował kryterium najniższej ceny. 4. Punkty w kryterium „Cena" zostaną obliczone na podstawie poniższego wzoru: Cena oferty najtańszej Liczba punktów = ---------- x 100 Cena oferty badanej 5. Końcowy wynik powyższego działania zostanie zaokrąglony do dwóch miejsc po przecinku zgodnie z zasadami arytmetyki. 6. Za najkorzystniejszą zostanie uznana oferta, która uzyska największą liczbę punktów. 7. W sytuacji, gdy Zamawiający nie będzie mógł dokonać wyboru najkorzystniejszej oferty ze względu na to, że zostały złożone oferty o takiej samej cenie, wezwie on Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych zawierających nową cenę. Wykonawcy, składając oferty dodatkowe, nie mogą zaoferować cen wyższych niż zaoferowane w uprzednio złożonych przez nich ofertach. 8. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert lub innych składanych dokumentów lub oświadczeń. Wykonawcy są zobowiązani do przedstawienia wyjaśnień w terminie wskazanym przez Zamawiającego. 9. Zamawiający wybiera najkorzystniejszą ofertą w terminie związania ofertą określonym w SWZ. 10. Jeżeli termin związania ofertą upłynie przed wyborem najkorzystniejszej oferty, Zamawiający wezwie Wykonawcą, którego oferta otrzymała najwyższą oceną, do wyrażenia, w wyznaczonym przez Zamawiającego terminie, pisemnej zgody na wybór jego oferty. 11. W przypadku braku zgody, o której mowa w ust. 9, oferta podlega odrzuceniu, a Zamawiający zwraca sią o wyrażenie takiej zgody do kolejnego Wykonawcy, którego oferta została najwyżej oceniona, chyba ze zachodzą przesłanki do unieważnienia postępowania.

5.1.11. Súťažné podklady

Adresa súťažných podkladov: https://ezamowienia.gov.pl

Ad hoc komunikačný kanál:

Názov: Portal e-Zamówienia

URL: https://ezamowienia.gov.pl

5.1.12. Podmienky verejného obstarávania

Podmienky predkladania:

Elektronické predkladanie: Povinná

Adresa na predkladanie: https://ezamowienia.gov.pl

Jazyky, v ktorých možno predložiť ponuky alebo žiadosti o účasť: poľština

Elektronický katalóg: Nie je povolená

Vyžaduje sa zdokonalený alebo kvalifikovaný elektronický podpis alebo elektronická pečať [v zmysle nariadenia (EÚ) č. 910/2014]

Varianty: Nie je povolená

Lehota na prijímanie ponúk: 18/08/2026 10:00:00 (UTC+02:00) východoeurópsky čas, stredoeurópsky letný čas

Doba, počas ktorej musí ponuka zostať platná: 90 Dni

Informácie o verejnom otváraní ponúk:

Dátum otvorenia: 18/08/2026 10:30:00 (UTC+02:00) východoeurópsky čas, stredoeurópsky letný čas

Miesto: https://ezamowienia.gov.pl

Podmienky zmluvy:

Plnenie zmluvy sa musí vykonať v rámci programov chránených pracovísk: Nie

Elektronická fakturácia: Povinná

Bude sa využívať elektronické objednávanie: nie
Bude sa využívať elektronická platba: áno

5.1.15. Techniky

Rámcová dohoda:

Žiadna rámcová dohoda

Informácie o dynamickom nákupnom systéme:

Žiadny dynamický nákupný systém

5.1.16. Ďalšie informácie, mediácia a preskúmanie

Organizácia pre preskúmanie: Krajowa Izba Odwoławcza
Informácie o lehotách na preskúmanie: Informacje o terminach odwołania: 1. Odwołanie wnosi się: 1) w przypadku zamówień, których wartość jest równa albo przekracza progi unijne, w terminie: a) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej, b) 15 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w lit. a; 2) w przypadku zamówień, których wartość jest mniejsza niż progi unijne, w terminie: a) 5 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej, b) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w lit. a. 2. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub konkurs lub wobec treści dokumentów zamówienia wnosi się w terminie: 1) 10 dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia dokumentów zamówienia na stronie internetowej, w przypadku zamówień, których wartość jest równa albo przekracza progi unijne; 2) 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub dokumentów zamówienia na stronie internetowej, w przypadku zamówień, których wartość jest mniejsza niż progi unijne. 3. Odwołanie w przypadkach innych niż określone w ust. 1 i 2 wnosi się w terminie: 1) 10 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia, w przypadku zamówień, których wartość jest równa albo przekracza progi unijne; 2) https://ted.europa.eu/TED Page 5/7 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia, w przypadku zamówień, których wartość jest mniejsza niż progi unijne. 4. Jeżeli zamawiający nie opublikował ogłoszenia o zamiarze zawarcia umowy lub mimo takiego obowiązku nie przesłał wykonawcy zawiadomienia o wyborze najkorzystniejszej oferty lub nie zaprosił wykonawcy do złożenia oferty w ramach dynamicznego systemu zakupów lub umowy ramowej, odwołanie wnosi się nie później niż w terminie: 1) 15 dni od dnia zamieszczenia w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania albo 30 dni od dnia publikacji w Dzienniku Urzędowym Unii Europejskiej ogłoszenia o udzieleniu zamówienia, a w przypadku udzielenia zamówienia w trybie negocjacji bez ogłoszenia albo zamówienia z wolnej ręki ogłoszenia o wyniku postępowania albo ogłoszenia o udzieleniu zamówienia, zawierającego uzasadnienie udzielenia zamówienia w trybie negocjacji bez ogłoszenia albo zamówienia z wolnej ręki; 2) 6 miesięcy od dnia zawarcia umowy, jeżeli zamawiający: a) nie opublikował w Dzienniku Urzędowym Unii Europejskiej ogłoszenia o udzieleniu zamówienia albo b) opublikował w Dzienniku Urzędowym Unii Europejskiej ogłoszenie o udzieleniu zamówienia, które nie zawiera uzasadnienia udzielenia zamówienia w trybie negocjacji bez ogłoszenia albo zamówienia z wolnej ręki; 3) miesiąca od dnia zawarcia umowy, jeżeli

zamawiający: a) nie zamieścił w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania albo b) zamieścił w Biuletynie Zamówień Publicznych ogłoszenie o wyniku postępowania, które nie zawiera uzasadnienia udzielenia zamówienia w trybie negocjacji bez ogłoszenia albo zamówienia z wolnej ręki.
Organizácia poskytujúca ďalšie informácie o postupy preskúmania: Krajowa Izba Odwoławcza
Organizácia prijímajúca žiadosti o účasť: PRZEDSIĘBIORSTWO KOMUNALNE SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
Organizácia spracúvajúca ponuky: PRZEDSIĘBIORSTWO KOMUNALNE SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

8. Organizácie

8.1. ORG-0001

Úradný názov: PRZEDSIĘBIORSTWO KOMUNALNE SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
Registračné číslo: NIP: 5440004192
Registračné číslo: REGON: 050243985
Poštová adresa: ul. ul. Armii Krajowej 26
Mesto: Siemiatycze
PSČ: 17-300
Nižšia územná jednotka krajiny (NUTS): Łomżyński (PL842)
Krajina: Poľsko
E-mail: sekretariat@pksiemiatycze.pl
Telefón: +4885 6552577
Internetová adresa: www.pksiemiatycze.pl
Roly tejto organizácie:
Kupujúci
Organizácia prijímajúca žiadosti o účasť
Organizácia spracúvajúca ponuky

8.1. ORG-0002

Úradný názov: Krajowa Izba Odwoławcza
Registračné číslo: NIP 5262239325
Poštová adresa: ul. Postępu 17a
Mesto: Warszawa
PSČ: 02676
Nižšia územná jednotka krajiny (NUTS): Miasto Warszawa (PL911)
Krajina: Poľsko
E-mail: odwolania@uzp.gov.pl
Telefón: +48 (22) 458 78 01
Fax: +48 458 78 00
Internetová adresa: https://www.gov.pl/web/uzp/kontakt2
Roly tejto organizácie:
Organizácia pre preskúmanie
Organizácia poskytujúca ďalšie informácie o postupy preskúmania

10. Zmena

Verzia prechádzajúceho oznámenia, ktorá sa má upraviť
:

ec2e6e82-aabf-48f7-8168-46261f4e1118-02
Hlavný dôvod zmeny
:
Oprava chyby vydavateľa

Informácie o oznámení

Identifikátor/verzia oznámenia: 87cfdb74-d23d-4d38-af7a-176e0bbd7d44 - 02
Typ formulára: Súťaž
Typ oznámenia: Oznámenie o vyhlásení verejného obstarávania alebo oznámenie o koncesii – štandardný režim
Podtyp oznámenia: 16
Dátum odoslania oznámenia: 23/07/2026 11:41:56 (UTC+02:00) východoeurópsky čas, stredoeurópsky letný čas
Jazyky, v ktorých je toto oznámenie oficiálne k dispozícii: poľština
Číslo uverejnenia oznámenia: 515394-2026
Číslo vydania série S úradného vestníka: 141/2026
Dátum uverejnenia: 24/07/2026