

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

Przedmiot zamówienia:

**„Dostawa sprzętu informatycznego w ramach realizacji projektu –
CyberKropla – Cyberbezpieczny Wodociąg w Darłowie”**

Nazwa Zamawiającego:

Gminny Zakład Użyteczności Publicznej Sp. z o. o.

Krupy 72, 76-150 Darłowo

NIP: 4990657295, REGON: 364588468

Nr telefonu: +48 605 211 777

E-mail: gzup@post.pl

Adres skrzynki ePUAP: /gzup/SkrytkaESP

Strona internetowa: www.gzup.gminadarlowo.pl

Strona prowadzonego postępowania:

<https://ezamowienia.gov.pl/mp-client/search/list/ocds-148610-7b681ed5-f2d2-4e52-9381-ea8a590406da>

Godziny pracy Zamawiającego (dni pracujące): od godz. 7:00 do godz. 15:00

ZATWIERDZAM

Prezes GZUP Sp. z o.o. – Tomasz Gondek

Krupy, dnia 10 sierpnia 2026 r.

SPIS TREŚCI

Rozdział I. Tryb udzielenia zamówienia publicznego oraz miejsca, w których zostało zamieszczone ogłoszenie o zamówieniu.

Rozdział II. Informacja dotycząca możliwości prowadzenia negocjacji.

Rozdział III. Opis przedmiotu zamówienia.

Rozdział IV. Termin wykonania zamówienia.

Rozdział V. Zamówienia częściowe oraz informacja o ofercie wariantowej.

Rozdział VI. Zamówienia podobne.

Rozdział VII. Informacja o podwykonawcach.

Rozdział VIII. Wykonawcy wspólnie ubiegający się o zamówienie.

Rozdział IX. Wykonawca mający siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej.

Rozdział X. Waluta w jakiej będą prowadzone rozliczenia związane z realizacją niniejszego zamówienia publicznego.

Rozdział XI. Podstawy wykluczenia z postępowania.

Rozdział XII. Warunki udziału w postępowaniu oraz sposób dokonywania oceny spełnienia tych warunków.

Rozdział XIII. Podmiotowe środki dowodowe.

Rozdział XIV. Wymagania dotyczące wadium.

Rozdział XV. Termin związania ofertą.

Rozdział XVI. 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.

Rozdział XVII. Informacje o sposobie komunikowania się zamawiającego z wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej, w przypadku zaistnienia jednej z sytuacji określonych w art. 65 ust. 1, art. 66 i art. 69 ustawy Pzp.

Rozdział XVIII. Opis sposobu przygotowania i składania ofert.

Rozdział XIX. Wymóg lub możliwość złożenia ofert w postaci katalogów elektronicznych lub dołączenia katalogów elektronicznych do oferty, w sytuacji określonej w art. 93 ustawy Pzp.

Rozdział XX. Termin składania ofert.

Rozdział XXI. Termin otwarcia ofert.

Rozdział XXII. Opis sposobu obliczania ceny.

Rozdział XXIII. Opis kryteriów oceny ofert wraz z podaniem wag tych kryteriów i sposobu oceny ofert.

Rozdział XXIV. Unieważnienie postępowania.

Rozdział XXV. Informacje o formalnościach, jakie zostaną dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego.

Rozdział XXVI. Wymagania dotyczące zabezpieczenia należytego wykonania umowy.

Rozdział XXVII. Istotne postanowienia umowy w sprawie zamówienia publicznego.

Rozdział XXVIII. Inne informacje.

Rozdział XXIX. Pouczenie o środkach ochrony prawnej przysługujących wykonawcom.

Rozdział XXX. Informacja o ochronie i przetwarzaniu danych osobowych.

ROZDZIAŁ I. TRYB UDZIELENIA ZAMÓWIENIA PUBLICZNEGO ORAZ MIEJSCA, W KTÓRYCH ZOSTAŁO ZAMIESZCZONE OGŁOSZENIE O ZAMÓWIENIU.

1. Postępowanie o udzielanie zamówienia publicznego prowadzone jest w trybie podstawowym na podstawie art. 275 pkt. 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2026, poz. 793 z późn. zm.) zwanej dalej ustawą Pzp oraz aktów wykonawczych do tej ustawy.
2. Miejsce publikacji ogłoszenia o zamówieniu:
 - a) Biuletyn Zamówień Publicznych;
 - b) strona prowadzonego postępowania:
<https://ezamowienia.gov.pl/mp-client/search/list/ocds-148610-7b681ed5-f2d2-4e52-9381-ea8a590406da>
na której udostępniane będą również zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia.

ROZDZIAŁ II. INFORMACJA DOTYCZĄCA MOŻLIWOŚCI PROWADZENIA NEGOCJACJI.

Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.

ROZDZIAŁ III. OPIS PRZEDMIOTU ZAMÓWIENIA.

1. Przedmiotem zamówienia jest dostawa sprzętu informatycznego w ramach realizacji projektu „CyberKropla – Cyberbezpieczny Wodociąg w Darłowie”.
2. Zamówienie współfinansowane jest w ramach Krajowego Planu Odbudowy i Zwiększania Odporności, Działanie C3.1.1 Cyberbezpieczeństwo – CyberPL. Konkurs grantowy o numerze KPOD.05.10-CW.01-001/25.
3. Przedmiot zamówienia podzielony został na sześć części:
 - 1) Część nr 1 – Dostawa serwera wraz z dyskami (wprowadzenie domeny Active Directory, wirtualizacja serwera);
 - 2) Część nr 2 – Dostawa przełącznika sieciowego;
 - 3) Część nr 3 – Dostawa urządzenia do archiwizacji danych;
 - 4) Część nr 4 – Dostawa zapory sieciowej;
 - 5) Część nr 5 – Dostawa Access Point Wi-Fi z centralnym zarządzaniem;
 - 6) Część nr 6 – Dostawa zasilacza awaryjnego (UPS).
4. Szczegółowy opis sprzętu informatycznego znajduje się w załącznikach nr 2a – 2f do SWZ.
5. Przedmiot dostawy powinien zostać dostarczony do siedziby Zamawiającego oraz oczyszczalni ścieków w Rusku.
6. **Wymagania ogólne:**
 - 1) O ile inaczej nie zaznaczono, wszelkie zapisy SWZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.
 - 2) Dostarczany sprzęt musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w styczniu 2025 r., wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie, pochodzić z oficjalnego kanału dystrybucyjnego. Przez stwierdzenie „fabrycznie nowy” należy rozumieć sprzęt opakowany oryginalnie (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Przez „wadę fizyczną” należy rozumieć również jakąkolwiek niezgodność ze opisem przedmiotu zamówienia.

- 3) Sprzęt musi być wyposażony we wszystkie niezbędne do jego działania i zapewnienia wymaganych funkcjonalności Sprzętu standardowe rozwiązania software'owe wraz z prawem do bezterminowego korzystania przez Zamawiającego z tych rozwiązań w takiej funkcji, jednakże w każdym przypadku nie krócej, niż przez czas, w jakim będzie technicznie możliwe używanie Sprzętu.
 - 4) Dokumenty gwarancyjne wystawiane i przekazywane przez Wykonawcę powinny być zgodne z zapisami SWZ.
 - 5) Oprogramowanie pochodzić będzie z legalnego, tj. akceptowanego przez producenta Oprogramowania kanału dystrybucji oraz zostanie udostępnione Zamawiającemu do korzystania na warunkach stosowanych lub akceptowanych przez takiego producenta.
7. **Kryteria równoważności:**
- 1) W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.
 - 2) W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm polskich lub europejskich, ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 5 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.
 - 3) Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w SWZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.

Wspólny Słownik Zamówień (CPV):

- 1) 30.20.00.00-1 – Urządzenia komputerowe;
- 2) 48.82.00.00-2 – Serwery;
- 3) 48.80.00.00-6 – Systemy i serwery informacyjne.

ROZDZIAŁ IV. TERMIN WYKONANIA ZAMÓWIENIA.

Termin realizacji zamówienia:

- 1) termin rozpoczęcia – **w dniu podpisania umowy;**
- 2) termin zakończenia – **60 dni od dnia podpisania umowy;**

ROZDZIAŁ V. ZAMÓWIENIA CZĘŚCIOWE ORAZ INFORMACJA O OFERCIE WARIANTOWEJ.

1. Zamawiający dopuszcza składanie ofert częściowych. Dopuszczalne jest składanie ofert zarówno na jedną jak i więcej części.
2. Zamawiający nie dopuszcza składania ofert wariantowych.

ROZDZIAŁ VI. ZAMÓWIENIA PODOBNE.

Zamawiający nie dopuszcza możliwości udzielenia zamówień polegających na powtórzeniu podobnych robót budowlanych zgodnych z przedmiotem zamówienia podanym powyżej.

ROZDZIAŁ VII. INFORMACJA O PODWYKONAWCACH.

1. Zamawiający nie zastrzega obowiązku osobistego wykonania przez wykonawcę kluczowych części zamówienia.
2. Zamawiający żąda wskazania części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez Wykonawców firm podwykonawców.
3. Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby wykonawca powoływał się, na zasadach określonych w art. 118 ustawy, w celu wykazania spełniania warunków udziału w postępowaniu, wykonawca jest obowiązany wykazać zamawiającemu, że proponowany inny podwykonawca lub wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż podwykonawca, na którego zasoby wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia.

ROZDZIAŁ VIII. WYKONAWCY WSPÓLNIE UBIEGAJĄCY SIĘ O ZAMÓWIENIE.

1. **Wykonawcy wspólnie ubiegający się o zamówienie:**
 - ponoszą solidarną odpowiedzialność za niewykonanie lub nienależyte wykonanie zobowiązania;
 - muszą ustanowić Pełnomocnika Wykonawców występujących wspólnie do reprezentowania ich w postępowaniu o udzielenie zamówienia publicznego albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia. Przyjmuje się, że pełnomocnictwo do podpisania oferty obejmuje pełnomocnictwo do poświadczenia za zgodność z oryginałem wszystkich dokumentów;
 - pełnomocnictwo musi jednocześnie wynikać z umowy lub z innej czynności prawnej, mieć formę pisemną, fakt ustanowienia Pełnomocnika musi wynikać z załączonych do oferty dokumentów, wszelka korespondencja prowadzona będzie z Pełnomocnikiem;
 - przed zawarciem umowy o niniejsze zamówienie publiczne, jeżeli oferta konsorcjum zostanie wybrana jako najkorzystniejsza, Zamawiający może wezwać do przedstawienia umowy regulującej współpracę tych Wykonawców.
 2. **Oferta wspólna, składana przez dwóch lub więcej Wykonawców powinna spełniać następujące wymagania:**
 - 1) musi być zgodna z postanowieniami SWZ;
 - 2) sposób składania dokumentów w przypadku składania oferty wspólnej:
 - a) **dokumenty wspólne, takie jak:**
 - oferta (**Załącznik nr 1 do SWZ**);
 - minimalne wymagania techniczno – użytkowe (**Załącznik nr 2a – 2f do SWZ**);
 - oświadczenie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO (**Załącznik nr 5 do SWZ**);
- podpisują wszyscy członkowie konsorcjum lub Pełnomocnik (Lider) w imieniu całego konsorcjum.**
- b) **dokumenty, takie jak:**
 - oświadczenie o spełnianiu warunków udziału w postępowaniu i braku podstaw do wykluczenia (**Załącznik nr 4 do SWZ**);
- składa każdy z partnerów konsorcjum w imieniu swojej firmy.**

ROZDZIAŁ IX. WYKONAWCA MAJĄCY SIEDZIBĘ LUB MIEJSCE ZAMIESZKANIA POZA TERYTORIUM RZECZPOSPOLITEJ POLSKIEJ.

Wykonawca mający siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej składa dokumenty zgodnie z przepisami rozporządzenia Ministra Rozwoju, Pracy i

Znak sprawy: ZP.2.2026

„Dostawa sprzętu informatycznego w ramach realizacji projektu – CyberKropla – Cyberbezpieczny Wodociąg w Darłowie”

Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od Wykonawcy (Dz. U. z 2020 r. poz. 2415).

ROZDZIAŁ X. WALUTA W JAKIEJ BĘDĄ PROWADZONE ROZLICZENIA ZWIĄZANE Z REALIZACJĄ NINIEJSZEGO ZAMÓWIENIA PUBLICZNEGO.

Wszelkie rozliczenia związane z realizacją niniejszego zamówienia dokonywane będą w walucie polskiej.

ROZDZIAŁ XI. PODSTAWY WYKLUCZENIA Z POSTĘPOWANIA.

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy:

- 1) nie podlegający wykluczeniu z postępowania na podstawie art. 108 ust 1 ustawy Pzp;
- 2) nie podlegający wykluczeniu z postępowania na podstawie art. 109 ust 1 ustawy Pzp;
 - a) który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, z wyjątkiem przypadku, o którym mowa w art. 108 ust. 1 pkt 3, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
 - b) który naruszył obowiązki w dziedzinie ochrony środowiska, prawa socjalnego lub prawa pracy:
 - będącego osobą fizyczną skazanego prawomocnie za przestępstwo przeciwko środowisku, o którym mowa w rozdziale XXII Kodeksu karnego lub za przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, o którym mowa w rozdziale XXVIII Kodeksu karnego, lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;
 - będącego osobą fizyczną prawomocnie ukaranego za wykroczenie przeciwko prawom pracownika lub wykroczenie przeciwko środowisku, jeżeli za jego popełnienie wymierzono karę aresztu, ograniczenia wolności lub karę grzywny;
 - wobec którego wydano ostateczną decyzję administracyjną o naruszeniu obowiązków wynikających z prawa ochrony środowiska, prawa pracy lub przepisów o zabezpieczeniu społecznym, jeżeli wymierzono tą decyzją karę pieniężną;
 - c) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo lub ukarano za wykroczenie, o którym mowa w pkt 2 lit. a lub b;
 - d) w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury;
 - e) który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał

- zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych dowodów;
- f) jeżeli występuje konflikt interesów w rozumieniu art. 56 ust. 2, którego nie można skutecznie wyeliminować w inny sposób niż przez wykluczenie wykonawcy;
 - g) który, z przyczyn leżących po jego stronie, w znacznym stopniu lub zakresie nie wykonał lub nienależycie wykonał albo długotrwale nienależycie wykonywał istotne zobowiązanie wynikające z wcześniejszej umowy w sprawie zamówienia publicznego lub umowy koncesji, co doprowadziło do wypowiedzenia lub odstąpienia od umowy, odszkodowania, wykonania zastępczego lub realizacji uprawnień z tytułu rękojmi za wady;
 - h) który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawianiu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub kryteria selekcji, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia, lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych podmiotowych środków dowodowych;
 - i) który bezprawnie wpływał lub próbował wpływać na czynności zamawiającego lub próbował pozyskać lub pozyskał informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia;
 - j) który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia;
- 3) nie podlegam wykluczeniu z postępowania na podstawie art. 7 ust 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t.j. Dz. U. z 2025, poz. 514 z późn. zm.).
2. Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia.
3. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2 i 5 lub art. 109 ust. 1 pkt 2-5 i 7-10, jeżeli udowodni Zamawiającemu, że spełnił łącznie następujące przesłanki:
- 1) naprawił lub zobowiązał się do naprawienia szkody wyrządzonej przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem, w tym poprzez zadośćuczynienie pieniężne;
 - 2) wyczerpująco wyjaśnił fakty i okoliczności związane z przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem oraz spowodowanymi przez nie szkodami, aktywnie współpracując odpowiednio z właściwymi organami, w tym organami ścigania, lub zamawiającym;
 - 3) podjął konkretne środki techniczne, organizacyjne i kadrowe, odpowiednie dla zapobiegania dalszym przestępstwom, wykroczeniom lub nieprawidłowemu postępowaniu, w szczególności:
 - a) zerwał wszelkie powiązania z osobami lub podmiotami odpowiedzialnymi za nieprawidłowe postępowanie wykonawcy,
 - b) zreorganizował personel,
 - c) wdrożył system sprawozdawczości i kontroli,
 - d) utworzył struktury audytu wewnętrznego do monitorowania przestrzegania przepisów, wewnętrznych regulacji lub standardów,
 - e) wprowadził wewnętrzne regulacje dotyczące odpowiedzialności i odszkodowań za nieprzestrzeganie przepisów, wewnętrznych regulacji lub standardów.

4. Zamawiający ocenia, czy podjęte przez Wykonawcę czynności, o których mowa w ust. 3, są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu wykonawcy. Jeżeli podjęte przez Wykonawcę czynności, o których mowa w ust. 3, nie są wystarczające do wykazania jego rzetelności, Zamawiający wyklucza wykonawcę.

ROZDZIAŁ XII. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ SPOSÓB DOKONYWANIA OCENY SPEŁNIENIA TYCH WARUNKÓW.

O udzielenie zamówienia mogą ubiegać się Wykonawcy spełniający warunki udziału w postępowaniu określone w SWZ i w art. 112 ustawy Pzp:

- 1) **posiadający zdolności do występowania w obrocie gospodarczym, tj.:**
Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie wykonawca zobowiązany jest wykazać w sposób szczególny. Ocena spełniania warunku udziału w postępowaniu Wykonawców zostanie dokonana w oparciu o zasadę spełnia – nie spełnia na podstawie oświadczenia załączonego do oferty, zgodnie z wymaganiami określonymi przez Zamawiającego w niniejszym postępowaniu;
- 2) **posiadający uprawnienia do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów, tj.:**
Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie wykonawca zobowiązany jest wykazać w sposób szczególny. Ocena spełniania warunku udziału w postępowaniu Wykonawców zostanie dokonana w oparciu o zasadę spełnia – nie spełnia na podstawie oświadczenia załączonego do oferty, zgodnie z wymaganiami określonymi przez Zamawiającego w niniejszym postępowaniu;
- 3) **znajdujący się w sytuacji ekonomicznej lub finansowej zapewniającej prawidłowe wykonanie zamówienia, tj.:**
Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie wykonawca zobowiązany jest wykazać w sposób szczególny. Ocena spełniania warunku udziału w postępowaniu Wykonawców zostanie dokonana w oparciu o zasadę spełnia – nie spełnia na podstawie oświadczenia załączonego do oferty, zgodnie z wymaganiami określonymi przez Zamawiającego w niniejszym postępowaniu;
- 4) **posiadający zdolności techniczne lub zawodowe zapewniające prawidłowe wykonanie zamówienia, tj.:**
Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie wykonawca zobowiązany jest wykazać w sposób szczególny. Ocena spełniania warunku udziału w postępowaniu Wykonawców zostanie dokonana w oparciu o zasadę spełnia – nie spełnia na podstawie oświadczenia załączonego do oferty, zgodnie z wymaganiami określonymi przez Zamawiającego w niniejszym postępowaniu.

ROZDZIAŁ XIII. PODMIOTOWE ŚRODKI DOWODOWE.

1. Do oferty Wykonawca dołącza oświadczenie o niepodleganiu wykluczeniu i spełnianiu warunków udziału w postępowaniu w zakresie wskazanym przez Zamawiającego.
2. Wzór oświadczenia, o którym mowa w ust. 1 stanowi **Załącznik nr 4 do SWZ**.
3. Oświadczenie, o którym mowa w ust. 1, stanowi dowód potwierdzający brak podstaw wykluczenia, spełnianie warunków udziału w postępowaniu na dzień składania ofert, tymczasowo zastępujący wymagane przez Zamawiającego podmiotowe środki dowodowe.
4. Jeżeli Wykonawca nie złożył oświadczenia, o którym mowa w art. 125 ust. 1 ustawy Pzp, podmiotowych środków dowodowych, o których mowa w art. 273 ustawy Pzp, innych dokumentów lub oświadczeń niezbędnych do przeprowadzenia postępowania,

oświadczenia lub dokumenty są niekompletne lub zawierają błędy, Zamawiający wzywa Wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia lub do udzielania wyjaśnień w terminie przez siebie wskazanym, chyba że mimo ich złożenia, uzupełnienia, poprawienia lub udzielenia wyjaśnień oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.

5. Jeżeli wykonawca nie złożył wymaganych pełnomocnictw albo złożył wadliwe pełnomocnictwa, zamawiający wzywa do ich złożenia w terminie przez siebie wskazanym, chyba że mimo ich złożenia oferta wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.

ROZDZIAŁ XIV. WYMAGANIA DOTYCZĄCE WADIUM.

Zamawiający nie wymaga wniesienia wadium.

ROZDZIAŁ XV. TERMIN ZWIĄZANIA OFERTĄ.

1. Wykonawca jest związany ofertą od dnia upływu terminu składania ofert **do dnia 3 października 2026 r.**
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą określonego w SWZ, Zamawiający przed upływem terminu związania ofertą zwraca się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazany przez niego okres, nie dłuższy niż 30 dni.
3. Przedłużenie terminu związania ofertą, o którym mowa w ust. 2, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.
4. W przypadku gdy Zamawiający żąda wniesienia wadium, przedłużenie terminu związania ofertą, o którym mowa w ust. 2, następuje wraz z przedłużeniem okresu ważności wadium albo jeżeli nie jest to możliwe, z wniesieniem nowego wadium na przedłużony okres związania ofertą.

ROZDZIAŁ XVI. 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 publicznego komunikacja między Zamawiającym, a Wykonawcami odbywa się przy użyciu Platformy e-Zamówienia, która jest dostępna pod adresem <https://ezamowienia.gov.pl>.
2. Korzystanie z Platformy e-Zamówienia jest bezpłatne.
3. Adres strony internetowej prowadzonego postępowania (link prowadzący bezpośrednio do widoku postępowania na Platformie e-Zamówienia): <https://ezamowienia.gov.pl/mp-client/search/list/ocds-148610-7b681ed5-f2d2-4e52-9381-ea8a590406da>.
4. Postępowanie można wyszukać również ze strony głównej Platformy e-Zamówienia (przycisk „Przeglądaj postępowania/konkursy”).
5. Identyfikator (ID) postępowania na Platformie e-Zamówienia: ocds-148610-7b681ed5-f2d2-4e52-9381-ea8a590406da.
6. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego musi posiadać konto podmiotu „Wykonawca” na Platformie e-Zamówienia. Szczegółowe informacje na temat zakładania kont podmiotów oraz zasady i warunki korzystania z Platformy e-Zamówienia określa **Regulamin Platformy e-Zamówienia**, dostępny na stronie internetowej <https://ezamowienia.gov.pl> oraz informacje zamieszczone w zakładce „Centrum Pomocy”.

7. Przeglądanie i pobieranie publicznej treści dokumentacji postępowania nie wymaga posiadania konta na Platformie e-Zamówienia ani logowania.
8. Sposób sporządzenia dokumentów elektronicznych lub dokumentów elektronicznych będących kopią elektroniczną treści zapisanej w postaci papierowej (cyfrowe odwzorowania) musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych.
9. Dokumenty elektroniczne, o których mowa w § 2 ust. 1 rozporządzenia Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych, sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, z uwzględnieniem rodzaju przekazywanych danych i przekazuje się jako załączniki. W przypadku formatów, o których mowa w art. 66 ust. 1 ustawy Pzp, ww. regulacje nie będą miały bezpośredniego zastosowania.
10. Informacje, oświadczenia lub dokumenty, inne niż wymienione w § 2 ust. 1 rozporządzenia Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych, przekazywane w postępowaniu sporządza się w postaci elektronicznej:
 - 1) w formatach danych określonych w przepisach rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (i przekazuje się jako załącznik), lub
 - 2) jako tekst wpisany bezpośrednio do wiadomości przekazywanej przy użyciu środków komunikacji elektronicznej (np. w treści wiadomości e-mail lub w treści **„Formularza do komunikacji”**).
11. Jeżeli dokumenty elektroniczne, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913 oraz z 2021 r. poz. 1655) wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem w nazwie pliku **„Dokument stanowiący tajemnicę przedsiębiorstwa”**.
12. Komunikacja w postępowaniu, z wyłączeniem składania ofert, odbywa się drogą elektroniczną za pośrednictwem formularzy do komunikacji dostępnych w zakładce **„Formularze”** (**„Formularze do komunikacji”**). Za pośrednictwem **„Formularzy do komunikacji”** odbywa się w szczególności przekazywanie wezwań i zawiadomień, zadawanie pytań i udzielanie odpowiedzi. Formularze do komunikacji umożliwiają również dołączenie załącznika do przesyłanej wiadomości (przycisk **„dodaj załącznik”**). W przypadku załączników, które są zgodnie z ustawą Pzp lub rozporządzeniem Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, mogą być opatrzone, zgodnie z wyborem wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia/podmiotu udostępniającego zasoby, podpisem typu zewnętrznego lub wewnętrznego. W zależności od rodzaju podpisu i jego typu (zewnętrzny, wewnętrzny) dodaje się uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny).
13. Możliwość korzystania w postępowaniu z **„Formularzy do komunikacji”** w pełnym zakresie wymaga posiadania konta **„Wykonawcy”** na Platformie e-Zamówienia oraz zalogowania się na Platformie e-Zamówienia. Do korzystania z **„Formularzy do komunikacji”** służących do zadawania pytań dotyczących treści dokumentów zamówienia wystarczające jest posiadanie tzw. konta uproszczonego na Platformie e-Zamówienia.

14. Wszystkie wysłane i odebrane w postępowaniu przez Wykonawcę wiadomości widoczne są po zalogowaniu w podglądzie postępowania w zakładce **„Komunikacja”**.
15. Maksymalny rozmiar plików przesyłanych za pośrednictwem **„Formularzy do komunikacji”** wynosi 150 MB (wielkość ta dotyczy plików przesyłanych jako załączniki do jednego formularza).
16. Minimalne wymagania techniczne dotyczące sprzętu używanego w celu korzystania z usług Platformy e-Zamówienia oraz informacje dotyczące specyfikacji połączenia określa **Regulamin Platformy e-Zamówienia**.
17. W przypadku problemów technicznych i awarii związanych z funkcjonowaniem Platformy e-Zamówienia użytkownicy mogą skorzystać ze wsparcia technicznego dostępnego pod numerem telefonu (32) 77 88 999 lub drogą elektroniczną poprzez formularz udostępniony na stronie internetowej <https://ezamowienia.gov.pl> w zakładce **„Zgłoś problem”**.
18. W szczególnie uzasadnionych przypadkach uniemożliwiających komunikację Wykonawcy i Zamawiającego za pośrednictwem Platformy e-Zamówienia, Zamawiający dopuszcza komunikację za pomocą poczty elektronicznej na adres e-mail: gzip@post.pl (nie dotyczy składania ofert).
19. Zamawiający wyznacza następujące osoby do komunikowania się z Wykonawcami:
 - 1) Daria Anna Dawid (tel. 692 500 244) – w zakresie procedury,
 - 2) Tomasz Gondek (tel. 605 400 175) – w zakresie przedmiotu zamówienia.

ROZDZIAŁ XVII. INFORMACJE O SPOSOBIE KOMUNIKOWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI W INNY SPOSÓB NIŻ PRZY UŻYCIU ŚRODKÓW KOMUNIKACJI ELEKTRONICZNEJ, W PRZYPADKU ZAISTNIENIA JEDNEJ Z SYTUACJI OKREŚLONYCH W ART. 65 UST. 1, ART. 66 I ART. 69.

Zamawiający nie przewiduje komunikowania się z wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej.

ROZDZIAŁ XVIII. OPIS SPOSOBU PRZYGOTOWANIA I SKŁADANIA OFERT.

1. Wykonawca składa ofertę za pośrednictwem zakładki **„Oferty/wnioski”**, widocznej w podglądzie postępowania po zalogowaniu się na konto Wykonawcy. Po wybraniu przycisku **„Złóż ofertę”** system prezentuje okno składania oferty umożliwiające przekazanie dokumentów elektronicznych, w którym znajdują się dwa pola drag&drop (**„przeciągnij”** i **„upuść”**) służące do dodawania plików.
2. Wykonawca dodaje wybrany z dysku i uprzednio podpisany **„Formularz oferty”** w pierwszym polu (**„Wypełniony formularz oferty”**). W kolejnym polu (**„Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”**) wykonawca dodaje pozostałe pliki stanowiące ofertę lub składane wraz z ofertą.
3. Jeżeli wraz z ofertą składane są dokumenty zawierające tajemnicę przedsiębiorstwa wykonawcy, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zaznaczeniem w nazwie pliku **„Dokument stanowiący tajemnicę przedsiębiorstwa”**. Zarówno załącznik stanowiący tajemnicę przedsiębiorstwa jak i uzasadnienie zastrzeżenia tajemnicy przedsiębiorstwa należy dodać w polu **„Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę”**.
4. **Formularz ofertowy** podpisuje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym w formacie PAdES typ wewnętrzny.
5. **Pozostałe dokumenty** wchodzące w skład oferty lub składane wraz z ofertą, które są zgodnie z ustawą Pzp lub rozporządzeniem Prezesa Rady Ministrów w sprawie wymagań

- dla dokumentów elektronicznych opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, mogą być zgodnie z wyborem wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia/podmiotu udostępniającego zasoby opatrzone podpisem typu zewnętrznego lub wewnętrznego. W zależności od rodzaju podpisu i jego typu (zewnętrzny, wewnętrzny) w polu „**Załączniki i inne dokumenty przedstawione w ofercie przez Wykonawcę**” dodaje się uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny).
6. W przypadku przekazywania dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku odpowiednio kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
 7. System sprawdza, czy złożone pliki są podpisane i automatycznie je szyfruje, jednocześnie informując o tym wykonawcę. Potwierdzenie czasu przekazania i odbioru oferty znajduje się w Elektronicznym Potwierdzeniu Przesłania (EPP) i Elektronicznym Potwierdzeniu Odebrania (EPO). EPP i EPO dostępne są dla zalogowanego Wykonawcy w zakładce „**Oferty/Wnioski**”.
 8. Oferta może być złożona tylko do upływu terminu składania ofert.
 9. Wykonawca może przed upływem terminu składania ofert wycofać ofertę. Wykonawca wycofuje ofertę w zakładce „**Oferty/wnioski**” używając przycisku „**Wycofaj ofertę**”.
 10. Maksymalny łączny rozmiar plików stanowiących ofertę lub składanych wraz z ofertą to 250 MB.

ROZDZIAŁ XIX. WYMÓG LUB MOŻLIWOŚĆ ZŁOŻENIA OFERT W POSTACI KATALOGÓW ELEKTRONICZNYCH LUB DOŁĄCZENIA KATALOGÓW ELEKTRONICZNYCH DO OFERTY, W SYTUACJI OKREŚLONEJ W ART. 93 USTAWY PZP

Zamawiający dopuszcza możliwość dołączenia katalogów elektronicznych do składanej oferty.

ROZDZIAŁ XX. TERMIN SKŁADANIA OFERT.

1. Ofertę wraz z wymaganymi załącznikami należy złożyć w terminie **w terminie do dnia 4 września 2026 roku, do godz. 13:30.**
2. Wykonawca może złożyć tylko jedną ofertę.
3. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.

ROZDZIAŁ XXI. TERMIN OTWARCIA OFERT.

1. Otwarcie ofert nastąpi w dniu **4 września 2026 roku, o godz. 14:00.**
2. Niezwłocznie po otwarciu ofert Zamawiający udostępni 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.

ROZDZIAŁ XXII. OPIS SPOSOBU OBLICZANIA CENY.

1. Wykonawca powinien dokonać wyceny wszystkich elementów związanych z przedmiotem zamówienia opisanym w SWZ z uwzględnieniem wszelkich kosztów, opłat i podatków zgodnie z obowiązującymi przepisami wraz z podatkiem VAT.
2. Ceny w ofercie muszą być podane do dwóch miejsc po przecinku.
3. Ceny w ofercie muszą zawierać wszystkie koszty związane z realizacją przedmiotowego zamówienia.
4. Zamawiający nie dopuszcza możliwości zmiany wynagrodzenia w okresie trwania umowy.

ROZDZIAŁ XXIII. OPIS KRYTERIÓW OCENY OFERT WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT.

Kryterium	Waga kryterium
Cena oferty	60 %
Termin płatności faktury (nie krótszy niż 7 dni i nie dłuższy niż 30 dni)	40 %
Łącznie	100 %

1. Maksymalna liczba punktów w danym kryterium równa jest określonej wadze kryterium w %.
2. Ocena łączna stanowi sumę punktów uzyskanych w ramach wszystkich kryteriów. Uzyskana liczba punktów zaokrąglona będzie do drugiego miejsca po przecinku.
3. Przyznawanie liczby punktów poszczególnym ofertom będzie się odbywać według następujących zasad:

a) Cena oferty.

Ocenie zostanie poddana cena brutto oferty obliczona przez Wykonawcę zgodnie z przepisami prawa – podana w Formularzu oferty (stanowiącym Załącznik nr 1 do SWZ). Liczba punktów, którą można uzyskać w tym kryterium zostanie obliczona według wzoru:

$$\text{liczba punktów} = \frac{\text{najniższa cena brutto spośród złożonych ofert}}{\text{cena brutto oferty ocenianej}} \times 60 \text{ pkt.}$$

b) Termin płatności faktury.

Termin płatności nie krótszy niż 7 dni i nie dłuższy niż 30 dni od dnia przedłożenia Zamawiającemu prawidłowo wystawionej faktury VAT. Zamawiający dokona stosownego obliczenia na podstawie wypełnionego formularza oferty (stanowiącego załącznik nr 1 do SWZ) i złożonej w nim deklaracji Wykonawcy o terminie płatności. Liczba punktów, jaką można uzyskać w tym kryterium zostanie obliczona na podstawie poniższego wzoru:

$$\text{liczba punktów} = \frac{\text{termin płatności w ofercie ocenianej}}{\text{najdłuższy termin płatności spośród złożonych ofert}} \times 40 \text{ pkt.}$$

4. Zamówienie zostanie udzielone Wykonawcy, który uzyska najwyższą liczbę punktów w wyniku oceny oferty.
5. Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający wybiera spośród tych ofert ofertę, która otrzymała najwyższą ocenę w kryterium o najwyższej wadze.
6. Jeżeli oferty otrzymały taką samą ocenę w kryterium o najwyższej wadze, Zamawiający wybiera ofertę z najniższą ceną.
7. Jeżeli nie można dokonać wyboru oferty w sposób, o którym mowa w ust. 6, Zamawiający wzywa Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych zawierających nową cenę.
8. Wykonawcy, składając oferty dodatkowe, nie mogą oferować cen wyższych niż zaoferowane w uprzednio złożonych przez nich ofertach.
9. Komisja Przetargowa sprawdzi, czy oferta spełnia warunki i wymogi ustawy Pzp i SWZ.
10. W toku badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert.
11. Na podstawie kryteriów oceny ofert Zamawiający będzie oceniał każdą spośród ofert nie podlegających odrzuceniu i wybierze ofertę najkorzystniejszą.
12. Zamawiający odrzuci ofertę, jeżeli zajdzie co najmniej jedna z przesłanek wymienionych w art. 226 ust. 1 ustawy Pzp.
13. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający informuje równocześnie Wykonawców, którzy złożyli oferty, podając uzasadnienie faktyczne i prawne, o:
 - 1) wyborze najkorzystniejszej oferty, podając nazwę albo imię i nazwisko, siedzibę albo miejsce zamieszkania, jeżeli jest miejscem wykonywania działalności wykonawcy, którego ofertę wybrano, oraz nazwy albo imiona i nazwiska, siedziby albo miejsca zamieszkania, jeżeli są miejscami wykonywania działalności Wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację;
 - 2) Wykonawcach, których oferty zostały odrzucone.
14. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego lub nie wnosi wymaganego zabezpieczenia należytego wykonania umowy, Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców oraz wybrać najkorzystniejszą ofertę albo unieważnić postępowanie.

ROZDZIAŁ XXIV. UNIEWAŻNIENIE POSTĘPOWANIA.

1. Zamawiający unieważni postępowanie o udzielenie zamówienia w przypadkach określonych w art. 255 i 256 ustawy Pzp.
2. O unieważnieniu postępowania o udzielenie zamówienia Zamawiający zawiadamia równocześnie Wykonawców, którzy złożyli oferty podając uzasadnienie faktyczne i prawne.
3. W przypadku unieważnienia postępowania o udzielenie zamówienia z przyczyn leżących po stronie Zamawiającego, Wykonawcom, którzy złożyli oferty niepodlegające odrzuceniu, przysługuje roszczenie o zwrot uzasadnionych kosztów uczestnictwa w tym postępowaniu, w szczególności kosztów przygotowania oferty.
4. W przypadku unieważnienia postępowania o udzielenie zamówienia Zamawiający niezwłocznie zawiadamia Wykonawców, którzy ubiegali się o udzielenie zamówienia w tym postępowaniu, o wszczęciu kolejnego postępowania, które dotyczy tego samego przedmiotu zamówienia lub obejmuje ten sam przedmiot zamówienia.

ROZDZIAŁ XXV. INFORMACJE O FORMALNOŚCIACH, JAKIE ZOSTANĄ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO.

1. W zawiadomieniu o wyborze oferty najkorzystniejszej Zamawiający poinformuje Wykonawcę o terminie i miejscu zawarcia umowy.
2. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego lub nie wnosi wymaganego zabezpieczenia należytego wykonania umowy, Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców oraz wybrać najkorzystniejszą ofertę albo unieważnić postępowanie.

ROZDZIAŁ XXVI. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY.

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

ROZDZIAŁ XXVII. ISTOTNE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO.

1. Istotne postanowienia umowy zawarte zostały w projekcie umowy **Załącznik nr 3 do SWZ**.
2. Zamawiający przewiduje możliwość dokonania zmiany postanowień umowy na podstawie art. 455 ustawy Prawo zamówień publicznych, które zostaną wyrażone w formie pisemnego aneksu pod rygorem nieważności i mogą nastąpić wyłącznie w następujących sytuacjach:
 - 1) zmiany terminu wykonania umowy, w przypadku:
 - a) wystąpienia okoliczności, których nie można było przewidzieć w chwili zawarcia umowy,
 - b) wstrzymanie realizacji przedmiotu umowy przez Zamawiającego nie wynikające z przyczyn leżących po stronie Wykonawcy,
 - c) wyrażenia zgody przez Zamawiającego na skrócenie terminu realizacji,
 - 2) w zakresie zmiany wynagrodzenia, zwłaszcza w sytuacji zmiany stawki obowiązującego podatku od towarów i usług (VAT).
3. Warunkiem dokonania zmian, o których mowa w ust. 2, jest złożenie wniosku przez stronę inicjującą zmianę zawierającego:
 - 1) opis propozycji zmiany,
 - 2) uzasadnienie zmiany,
 - 3) obliczenie kosztów zmiany zgodnie z zasadami określonymi w umowie, jeżeli zmiana będzie miała wpływ na wynagrodzenie Wykonawcy,
 - 4) opis wpływu zmiany na harmonogram realizacji i fakturowania oraz termin wykonania umowy.
4. Wykonawca nie będzie uprawniony do żądania przedłużenia terminu wykonania umowy i zwiększenia wynagrodzenia, jeżeli zmiana jest wymuszona uchybieniem czy naruszeniem umowy przez Wykonawcę – w takim przypadku koszty dodatkowe związane takimi zmianami ponosi Wykonawca.
5. Powyższe zmiany nie mogą być niekorzystne dla Zamawiającego.
6. Poza przypadkami opisanymi w niniejszym paragrafie, zmiana umowy może nastąpić w przypadkach przewidzianych w art. 455 ust. 1 pkt. 2 – 4 i ust. 2 ustawy Prawo zamówień publicznych.

ROZDZIAŁ XXVIII. INNE INFORMACJE.

Nie przewiduje się:

- 1) zawarcia umowy ramowej,
- 2) ustanowienia dynamicznego systemu zakupów,
- 3) wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej.

ROZDZIAŁ XXIX. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCOM.

Wykonawcom, których interes prawny w uzyskaniu zamówienia doznał lub może doznać uszczerbku w wyniku naruszenia przez Zamawiającego przepisów ustawy, przepisów wykonawczych jak też postanowień niniejszej SWZ przysługują środki ochrony prawnej przewidziane w Dziale IX (art. 505-590) ustawy Pzp.

ROZDZIAŁ XXX. INFORMACJA O OCHRONIE I PRZETWARZANIU DANYCH OSOBOWYCH.

1. Zamawiający udostępnia dane osobowe, o których mowa w art. 10 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, z późn. zm.), zwanego dalej „RODO”, w celu umożliwienia korzystania za środków ochrony prawnej, o których mowa w ustawie, do upływu terminu na ich wniesienie.
2. Zgodnie z art. 13 ust. 1 i 2 RODO, zamawiający informuje, że:
 - 1) administratorem a w przypadku zamówień współfinansowanych ze środków UE (jeżeli dotyczy) również podmiotem przetwarzającym wszelkie dane osobowe osób fizycznych związanych z niniejszym postępowaniem jest Gminny Zakład Użyteczności Publicznej Sp. z o. o. Krupy 72, 76-150 Darłowo,
 - 2) kontakt do inspektora ochrony danych osobowych w Gminnym Zakładzie Użyteczności Publicznej Sp. z o. o. Krupy 72, 76-150 Darłowo, tel. 605-211-777, adres e-mail: iod@gzup.gminadarlowo.pl,
 - 3) dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie niniejszego zamówienia,
 - 4) odbiorcami ww. danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy oraz umowy dofinansowania (jeżeli dotyczy),
 - 5) ww. dane osobowe będą przechowywane odpowiednio:
 - a) przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia publicznego albo przez cały okres obowiązywania umowy w sprawie zamówienia publicznego - jeżeli okres obowiązywania umowy przekracza 4 lata;
 - b) do czasu przeprowadzania archiwizacji dokumentacji – w zakresie określonym w przepisach o archiwizacji,
 - 6) obowiązek podania danych osobowych jest wymogiem ustawowym określonym w przepisach ustawy, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy,
 - 7) w odniesieniu do danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO,
 - 8) osoba fizyczna, której dane osobowe dotyczą posiada:
 - a) na podstawie art. 15 RODO prawo dostępu do ww. danych osobowych. W przypadku korzystania przez osobę, której dane osobowe są przetwarzane przez zamawiającego, z uprawnienia, o którym mowa w art. 15 ust. 1-3 RODO, zamawiający może żądać

od osoby, występującej z żądaniem wskazania dodatkowych informacji, mających na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia;

- b) na podstawie art. 16 RODO prawo do sprostowania ww. danych osobowych (skorzystanie z prawa do sprostowania lub uzupełnienia nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia ani zmianą postanowień umowy w sprawie zamówienia publicznego w zakresie niezgodnym z ustawą oraz nie może naruszać integralności protokołu postępowania oraz jego załączników);
 - c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych. Zgłoszenie żądania ograniczenia przetwarzania nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania. W przypadku, gdy wniesienie żądania dotyczącego prawa, o którym mowa w art. 18 ust. 1 RODO, spowoduje ograniczenie przetwarzania danych zawartych w protokole postępowania lub załącznikach do tego protokołu, od dnia zakończenia postępowania o udzielenie zamówienia zamawiający nie udostępnia tych danych, chyba, że zachodzą przesłanki, o których mowa w art. 18 ust. 2 RODO;
 - d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy przetwarzanie danych osobowych narusza przepisy RODO,
- 9) osobie fizycznej, której dane osobowe dotyczą nie przysługuje:
- a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
 - b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
 - c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania danych osobowych jest art. 6 ust. 1 lit. c RODO.

FORMULARZ OFERTY

Gminny Zakład Użyteczności
Publicznej Sp. z o. o.
Krupy 72
76-150 Darłowo

Odpowiadając na ogłoszenie dotyczące zamówienia pn.: „Dostawa sprzętu informatycznego w ramach realizacji projektu – CyberKropla – Cyberbezpieczny Wodociąg w Darłowie” oferujemy wykonanie przedmiotu zamówienia zgodnie z wymogami zawartymi w Specyfikacji Warunków Zamówienia za cenę:

Część nr 1

Wartość netto zamówienia: zł,

VAT - %: zł,

Wartość brutto zamówienia: zł,

Słownie:,

**Cena oferty brutto jest ceną ostateczną obejmującą wszystkie koszty i składniki związane z realizacją zamówienia w tym podatek VAT.*

Termin płatności faktury:dni (nie krótszy niż 7 dni i nie dłuższy niż 30 dni).

Część nr 2

Wartość netto zamówienia: zł,

VAT - %: zł,

Wartość brutto zamówienia: zł,

Słownie:,

**Cena oferty brutto jest ceną ostateczną obejmującą wszystkie koszty i składniki związane z realizacją zamówienia w tym podatek VAT.*

Termin płatności faktury:dni (nie krótszy niż 7 dni i nie dłuższy niż 30 dni).

Część nr 3

Wartość netto zamówienia: zł,

VAT - %: zł,

Wartość brutto zamówienia: zł,

Słownie:,

**Cena oferty brutto jest ceną ostateczną obejmującą wszystkie koszty i składniki związane z realizacją zamówienia w tym podatek VAT.*

Termin płatności faktury:dni (nie krótszy niż 7 dni i nie dłuższy niż 30 dni).

Część nr 4

Wartość netto zamówienia: zł,

VAT - %: zł,

Wartość brutto zamówienia: zł,

Słownie:,

****Cena oferty brutto jest ceną ostateczną obejmującą wszystkie koszty i składniki związane z realizacją zamówienia w tym podatek VAT.***

Termin płatności faktury:dni (nie krótszy niż 7 dni i nie dłuższy niż 30 dni).

Część nr 5

Wartość netto zamówienia: zł,

VAT - %: zł,

Wartość brutto zamówienia: zł,

Słownie:,

****Cena oferty brutto jest ceną ostateczną obejmującą wszystkie koszty i składniki związane z realizacją zamówienia w tym podatek VAT.***

Termin płatności faktury:dni (nie krótszy niż 7 dni i nie dłuższy niż 30 dni).

Część nr 6

Wartość netto zamówienia: zł,

VAT - %: zł,

Wartość brutto zamówienia: zł,

Słownie:,

****Cena oferty brutto jest ceną ostateczną obejmującą wszystkie koszty i składniki związane z realizacją zamówienia w tym podatek VAT.***

Termin płatności faktury:dni (nie krótszy niż 7 dni i nie dłuższy niż 30 dni).

Nazwa i adres podmiotu składającego ofertę:

.....

NIP **REGON**
Adres, na który Zamawiający powinien przysłać ewentualną korespondencję:

.....

Osoba wyznaczona do kontaktów z Zamawiającym:

.....

Numer telefonu:
Numer faksu:
e-mail

1. Oświadczam, że podmiot, który reprezentuję to (zaznaczyć właściwe):
 - ☐ mikroprzedsiębiorstwo,
 - ☐ małe przedsiębiorstwo,
 - ☐ średnie przedsiębiorstwo,
 - ☐ jednoosobowa działalność gospodarcza,
 - ☐ osoba fizyczna nieprowadząca działalności gospodarczej,
 - ☐ inny rodzaj.
2. Oświadczamy, że:
 - 1) zapoznaliśmy się z warunkami podanymi przez Zamawiającego w SWZ i nie wnosimy do nich żadnych zastrzeżeń,
 - 2) uzyskaliśmy wszelkie niezbędne informacje do przygotowania oferty i wykonania zamówienia.
 - 3) akceptujemy istotne postanowienia umowy oraz termin realizacji przedmiotu zamówienia podany przez Zamawiającego,
 - 4) uważamy się za związanych niniejszą ofertą od dnia upływu terminu składania ofert do dnia wskazanego w Rozdziale XV ust. 1.
3. W przypadku udzielenia nam zamówienia zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.
4. Do oferty dołączono:
 - Minimalne wymagania techniczno – użytkowe – Załącznik nr (2a – 2f) do SWZ.
 - Oświadczenie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO.
 -,
 -,
 -,
 -,
 -,
 -,

....., dn.

.....
*Podpis/-y osób uprawnionych do składania świadczeń
 woli w imieniu Wykonawcy oraz pieczętka imienna /
 pieczętka*

MINIMALNE WYMAGANIA TECHNICZNO – UŻYTKOWE

Część nr 1 – Dostawa serwera wraz z dyskami (wprowadzenie domeny Active Directory, wirtualizacja serwera)

Serwer – 1 szt.:

Producent	
Typ/model	
Numer produktu	

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie
Obudowa	Do instalacji w szafie Rack 19”, wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość instalacji ramienia do zarządzania kablami	
Procesor	Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – 12. Minimalna częstotliwość pracy procesora 2.2GHz. Minimalna ilość kanałów procesora – 8. Ilość kości pamięci na kanał – 2. Wynik wydajności procesora nie powinien być niższy niż 422 punkty base w teście SPECrate 2017 Integer w konfiguracji jednoprocessorowej, opublikowanym przez SPEC.org (www.spec.org), dla serwera oferowanego producenta.	
Liczba zainstalowanych procesorów	1	
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów Intel Xeon wykonujących 64-bitowe instrukcje	
Pamięć operacyjna	Zainstalowane minimum 128GB pamięci RAM o częstotliwości 6400MHz. Pamięć zainstalowana w kościach 32GB Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.	
Zabezpieczenie pamięci	Memory mirroring, ECC, SDDC, ADDDC	
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.	
Rozbudowa dysków	W chwili dostawy serwer musi posiadać zainstalowane minimum 4 sztuki dysków 960GB Read Intensive SATA 6Gb HS SSD v2 sterowanych kartą SAS/SATA 12Gb HBA. Wymagany jest wewnętrzny slot na kartę Micro SD.	
Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 1300W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.	
Interfejsy sieciowe	Zainstalowana przynajmniej jedna czteroportowa karta 10Gbase-T. Wymagana funkcjonalność portów: sprzętowa obsługa	

Znak sprawy: ZP.2.2026

„Dostawa sprzętu informatycznego w ramach realizacji projektu – CyberKropla – Cyberbezpieczny Wodociąg w Darłowie”

	protokołów VXLAN, NVGRE, GENEVE. Karta nie może zajmować żadnego ze slotów PCIe wymienionych w punkcie Sloty I/O. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.	
Sloty I/O	Serwer w momencie dostawy powinien posiadać 1 slot PCIe Gen5 x8 w pełnej wysokości, 1 slot OCP Gen5 oraz dedykowane połączenie PCIe dla kontrolera dyskowego niezajmujące slotów PCIe.	
Dodatkowe porty	Z tyłu obudowy: 2x USB 3, 1x VGA, 1x RJ-45 do zarządzania serwerem. Wewnątrz obudowy: Możliwość instalacji portu USB 3.	
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1	
Zarządzanie	Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płycie I/O (wspomnianej w sekcji Dodatkowe Porty). • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna) • Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, użycie cpu, użycie pamięci oraz komponentów I/O, lokalizacja • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. • Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3 • Update systemowego firmware • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zapis video zdalnych sesji • Podmontowanie lokalnych mediów z wykorzystaniem Java client • Przekierowanie konsoli szeregowej przez IPMI • Zrzut ekranu w momencie zawieszenia systemu • Możliwość przejęcia zdalnego ekranu • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH • Wyświetlanie danych aktualnych i historycznych dla użycia energii oraz temperatury serwera • Możliwość mapowania obrazów ISO z lokalnego dysku operatora • Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS • Możliwość jednoczesnej pracy do 6 użytkowników przez	

Znak sprawy: ZP.2.2026

„Dostawa sprzętu informatycznego w ramach realizacji projektu – CyberKropla – Cyberbezpieczny Wodociąg w Darłowie”

	wirtualną konsolę - wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API - Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. - Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. - Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. - Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. - Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200. Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające: - zarządzanie infrastrukturą serwerów i storage bez udziału dedykowanego agenta, - przedstawianie graficznej reprezentacji zarządzanych urządzeń, - możliwość skalowania do minimum 1000 urządzeń, - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2, - wsparcie dla certyfikatów SSL tzw. self-signed oraz zewnętrznych, - udostępnianie szybkiego podglądu stanu środowiska, - udostępnianie podsumowania stanu dla każdego urządzenia, - tworzenie alertów przy zmianie stanu urządzenia, - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, - konsola zarządzania oparta o HTML 5, - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja, - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie	
--	--	--

Znak sprawy: ZP.2.2026

„Dostawa sprzętu informatycznego w ramach realizacji projektu – CyberKropla – Cyberbezpieczny Wodociąg w Darłowie”

	producenta oferowanego rozwiązania, - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeniami, - definiowanie roli użytkowników oprogramowania, - obsługa REST API oraz Windows PowerShell, - obsługa SNMP, SYSLOG, Email Forwarding, - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML, - obsługa tzw. Forward Secrecy w komunikacji z zarządzanymi urządzeniami, - przedstawianie historycznych aktywności użytkowników, - blokowanie możliwości podłączenia innego systemu zarządzania do urządzeń zarządzanych, - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv, - Obsługa NTP, - przesyłanie alertów do konsoli firm trzecich, - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń), - instalowanie systemów operacyjnych oraz wirtualizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie, - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych. Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.	
Funkcje zabezpieczeń	Hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform Firmware Resiliency (PFR). Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Możliwość włączania i wyłączania portów USB na obudowie z poziomu karty zarządzania. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji.	
Urządzenia hot	Dyski twarde, zasilacze, wentylatory.	

Znak sprawy: ZP.2.2026

„Dostawa sprzętu informatycznego w ramach realizacji projektu – CyberKropla – Cyberbezpieczny Wodociąg w Darłowie”

swap		
Obsługa	Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ów PCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych.	
Diagnostyka	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID.	
Systemy operacyjne	Kompatybilny z: Microsoft Windows Server 2022, 2025; Red Hat Enterprise Linux 9.x; SUSE Linux Enterprise Server 15 SP6; VMware vSphere (ESXi) 8.0 U3; Ubuntu 22.04, 24.04 Wraz z serwerem powinno zostać dostarczone oprogramowanie Microsoft Windows Server 2025 Standard w licencji pokrywającej wszystkie rdzenie fizyczne procesorów zainstalowanych w serwerze.	
Waga	Maximum: 20 kg	
Gwarancja	36 miesięcy gwarancji producenta z reakcją NBD. Dyski pozostają własnością Zamawiającego. Możliwość wykupienia dodatkowego wsparcia, świadczonego przez producenta, z gwarantowanym czasem naprawy w ciągu 24 godzin. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalni jak i wydajnościowo wymagane powyżej maszyny. Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera.	

MINIMALNE WYMAGANIA TECHNICZNO – UŻYTKOWE

Część nr 2 – Dostawa przełącznika sieciowego

Przełącznik dystrybucyjny warstwy 3 klasy Enterprise – 1 szt.:

Producent	
Typ/model	
Numer produktu	

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie
Przedmiot zamówienia	Przedmiotem zamówienia jest dostawa przełącznika sieciowego klasy Enterprise przeznaczonego do pracy w warstwie dystrybucyjnej lub rdzeniowej sieci LAN. Urządzenie musi zapewniać wysoką dostępność, rozbudowane funkcje automatyzacji zarządzania, zaawansowane mechanizmy bezpieczeństwa oraz możliwość budowy odpornej na awarie infrastruktury sieciowej. Dopuszcza się rozwiązania równoważne spełniające wszystkie wymagania funkcjonalne i techniczne określone w niniejszym OPZ.	
Interfejsy	Przełącznik musi posiadać: • 24 porty 10/100/1000Base-T RJ45, • wszystkie porty RJ45 muszą obsługiwać IEEE 802.3af oraz IEEE 802.3at PoE+, • minimum 4 porty SFP+ 1/10GbE, • możliwość wykorzystania portów uplink jako portów transmisyjnych lub stackujących, • możliwość rozbudowy poprzez dedykowany moduł rozszerzeń.	
Wydajność	• Switching Fabric: ≥ 288 Gb/s, • Forwarding Rate: ≥ 214 Mpps, • VLAN: ≥ 4094, • MAC Address Table: $\geq 64\ 000$, • Jumbo Frame: ≥ 13 KB, • LAG: ≥ 128.	
Wysoka dostępność	Urządzenie musi zapewniać: • tworzenie stosu minimum 8 urządzeń, • możliwość budowy stosu poprzez połączenia światłowodowe na duże odległości, • przepustowość stackingu minimum 40 Gb/s na urządzenie, • możliwość zwiększenia przepustowości stackingu do minimum 160 Gb/s, • szybkie przełączanie awaryjne stosu, • agregację portów pomiędzy różnymi urządzeniami stosu, • brak pojedynczego punktu awarii.	
Automatyzacja	Przełącznik musi posiadać natywne mechanizmy umożliwiające:	

Znak sprawy: ZP.2.2026

„Dostawa sprzętu informatycznego w ramach realizacji projektu – CyberKropla – Cyberbezpieczny Wodociąg w Darłowie”

sieci	- centralne zarządzanie wszystkimi urządzeniami sieci jako jednym logicznym środowiskiem, - automatyczne wykrywanie nowych urządzeń, - automatyczne wdrażanie konfiguracji, - automatyczne aktualizacje firmware, - automatyczne wykonywanie kopii konfiguracji, - automatyczne odtwarzanie konfiguracji po wymianie urządzenia, - szyfrowaną komunikację pomiędzy urządzeniami zarządzającymi, - możliwość wdrożenia rozwiązania typu Zero Touch Deployment.	
Monitoring światłowodów	Przełącznik musi posiadać natywną funkcję: - ciągłego monitorowania poziomu mocy optycznej, - wykrywania prób fizycznej ingerencji w tor światłowodowy, - automatycznego wyłączenia portu lub wygenerowania alarmu po wykryciu naruszenia, - monitorowania zarówno łączy transmisyjnych, jak i stackujących.	
Diagnostyka	Urządzenie musi posiadać: - Link Monitoring z pomiarem opóźnienia, jittera i strat pakietów, - możliwość definiowania progów alarmowych, - automatyczne uruchamianie akcji po wykryciu pogorszenia parametrów, - TDR, - DDM, - UDLD, - CFM, - RSPAN, - Port Mirroring.	
Mechanizmy redundancji	Wymagana obsługa: Ethernet Protection Switching Ring, G.8032 ERPS, Media Redundancy Protocol, BFD, STP, RSTP, MSTP, LACP.	
Routing	Przełącznik musi obsługiwać: IPv4, IPv6, OSPFv2, OSPFv3, BGP, RIP, RIPng, VRF Lite, ECMP, Policy Based Routing, Multicast IPv4 i IPv6.	
Bezpieczeństwo	Wymagane: IEEE 802.1X, MAC Authentication, Web Authentication, Tri-Authentication, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, ACL L2/L3/L4, MACSec, SSH, HTTPS, SCP, SFTP, RADIUS, TACACS+, BPDU Guard, Loop Protection.	
Integracja z siecią bezprzewodową	Urządzenie musi posiadać możliwość: - zarządzania punktami dostępowymi Wi-Fi z poziomu przełącznika, - automatycznej optymalizacji kanałów radiowych, - automatycznej regulacji mocy nadawczej, - prezentacji map pokrycia radiowego, - zarządzania siecią przewodową i bezprzewodową z jednego interfejsu administracyjnego.	

Znak sprawy: ZP.2.2026

„Dostawa sprzętu informatycznego w ramach realizacji projektu – CyberKropla – Cyberbezpieczny Wodociąg w Darłowie”

Zarządzanie	Obsługa: CLI, GUI, SNMP v1/v2/v3, NETCONF, RESTCONF, YANG, Syslog, USB, dedykowanego portu zarządzającego Ethernet, portu konsolowego.	
Zasilanie	Przełącznik musi posiadać: • redundantne zasilacze wymieniane podczas pracy, • redundantne wentylatory wymieniane podczas pracy, • możliwość zachowania zasilania PoE podczas restartu urządzenia, • możliwość budowy redundantnego budżetu PoE.	

MINIMALNE WYMAGANIA TECHNICZNO – UŻYTKOWE

Część nr 3 – Dostawa urządzenia do archiwizacji danych

Serwer NAS – 1 szt.:

Producent	
Typ/model	
Numer produktu	

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie
Procesor	Wielordzeniowy procesor osiągający wynik minimum 14900 punktów w teście PassMark.	
Obudowa	Typu rack o wysokości maksymalnie 2U wraz z szynami przesuwными umożliwiającymi montaż w szafie rack w zestawie.	
Pamięć RAM	Minimum 32GB ECC tego samego producenta, co serwer NAS. Nie zezwala się na stosowanie zamienników.	
Ilość obsługiwanych dysków	Minimum 12 dysków o maksymalnej pojemności dysku nie mniejszej niż 20TB każdy, po podłączeniu modułów rozszerzających minimum 36 dysków.	
Zainstalowane dyski	3 dyski SSD do serwera o pojemności minimum 1920GB każdy zgodne z listą kompatybilności oferowanego serwera NAS oraz charakteryzujące się następującymi parametrami: • typ dysku: SSD, • format dysku: 2.5”, • gwarancja: minimum 36 miesięcy NBD z możliwością pozostawienia uszkodzonego nośnika u Zamawiającego, • możliwość aktualizacji oprogramowania dysków HDD bezpośrednio z poziomu systemu operacyjnego serwera NAS podczas pracy.	
Interfejsy zarządzania	Minimum 1 port LAN do zarządzania poza pasmem (OOB).	
Interfejsy sieciowe	Minimum 2 port 10GbE RJ-45. Minimum 2 port 10GbE SFP+. Obsługa agregacji łączy.	
Porty	Minimum 2 porty USB 3.2. Minimum 1 gniazdo rozszerzenia służące do podłączania jednostek rozszerzających.	
Wskaźniki LED	Status, HDD, zasilanie, LAN	
Obsługa RAID	Podstawowy, RAID 0, 1, 5, 6, 10. Obsługa dysków zapasowych typu hot spare.	
Funkcje RAID	Możliwość zwiększania pojemności poprzez wymianę dysków na większe. Migracja poziomu RAID w trybie online dla minimum RAID 1 i RAID 5.	
Szyfrowanie	Możliwość szyfrowania wybranych udziałów sieciowych.	
Protokoły	SMB, NFS, FTP, WebDAV, iSCSI, SSH, SNMP	

Usługi	1. Serwer VPN, Windows ACL, Integracja z Windows Active Directory, Firewall, Serwer WWW, Serwer plików, Manager plików przez WebUI, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Usługa DDNS, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki, możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów. 2. Możliwość utworzenia klastra wysokiej dostępności (<i>ang. High Availability Cluster</i>) pracującego minimum w trybie aktywny - pasywny. Klaster musi obsługiwać w pełni automatyczne przełączanie awaryjne bez ingerencji administratora. W skład klastra muszą wchodzić co najmniej 2 urządzenia. 3. Tworzenie zadań i wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 11 lub nowszym z centralnej konsoli zarządzania dostępnej lokalnie oraz zdalnie, z możliwością przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 6 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Bez ograniczenia liczby podłączanych komputerów do systemu kopii zapasowej. 4. Wykonywanie kopii zapasowych maszyn wirtualnych ze środowisk takich jak VMware vSphere, VMware free ESXi oraz Microsoft Hyper-V 2016, 2019, 2022 (wraz z klastrami przełączania awaryjnego) z wykorzystaniem centralnego panelu zarządzania oraz dodatkowo: • Obsługa wszystkich typów i wersji sprzętu wirtualnego VMware, w tym 62TB VMDK. • Obsługa maszyn wirtualnych Hyper-V generacji 1 i 2, w tym dysków VHDX o pojemności 64 TB i wersji sprzętu wirtualnego od 5.0 do 9.0. • W przypadku tworzenia kopii zapasowych Microsoft Hyper-V wymagany jest wolumin systemowy hosta z co najmniej 512 MB wolnego miejsca w celu zainstalowania narzędzia do przenoszenia danych. • Kopia zapasowa oparta na obrazie tworzy kopie zapasowe całych urządzeń, w tym konfiguracji danych i systemu. • Kopia zapasowa bez agentów. • Korzystanie z funkcji VMware Changed Block Tracking i funkcji Hyper-V Resilient Change Tracking do wykonywania przyrostowej kopii zapasowej • Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowych. • Metody przywracania: Przywracanie całego urządzenia, przywracanie na poziomie plików/folderów i natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V lub wbudowanego wirtualizatora na serwerze NAS.	
--	--	--

Znak sprawy: ZP.2.2026
„Dostawa sprzętu informatycznego w ramach realizacji projektu – CyberKropla – Cyberbezpieczny Wodociąg w Darłowie”

	- W przypadku przywracania na poziomie plików w systemie operacyjnym gościa obsługiwane systemy plików systemu Windows to NTFS i FAT32, a obsługiwane systemy plików systemu Linux to NTFS, FAT32, ext3, I ext4. - Kopia zapasowa uwzględniające aplikacje dla maszyn wirtualnych VMware vSphere lub Microsoft Hyper-V działających w systemie Microsoft Windows 2003 SP1 lub nowszym (z wyjątkiem Nano Server z powodu braku architektury VSS). - Obsługa tworzenia kopii zapasowych systemów operacyjnych i aplikacji obsługiwanych przez rozwiązania VMware vSphere i Microsoft Hyper-V.	
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów, możliwość aktualizacji oprogramowania dysków twardych bezpośrednio z poziomu interfejsu zarządzania systemu operacyjnego serwera NAS bez potrzeby demontażu dysków.	
Język GUI	Polski	
Gwarancja i serwis	Minimum 36 miesięcy gwarancji świadczonej przez producenta lub autoryzowanego partnera serwisowego producenta działającej w trybie NBD na cały system złożony z serwera, dysków i akcesoriów z opcją pozostawienia uszkodzonego nośnika u Zamawiającego.	
Waga	Maksymalnie 16 kg (bez dysków).	
Typowy pobór mocy podczas pracy	Maksymalnie 200W	
Certyfikaty	Minimum CE	
System plików	Dyski wewnętrzne: BTRFS lub inny równoważny	
Szyfrowanie	Mechanizm szyfrowania sprzętowego	
Zasilacz	Zasilacz redundantny o mocy pozwalającej na bezproblemową pracę serwera NAS w przypadku pełnego obciążenia dyskami HDD, SSD oraz kartami rozszerzeń.	
Chłodzenie	Minimum 2 wentylatory z możliwością regulowania prędkości obrotowej oraz wymiany w urządzeniu podczas pracy.	

MINIMALNE WYMAGANIA TECHNICZNO – UŻYTKOWE

Część nr 4 – Dostawa zapory sieciowej

UTM do siedziby Zamawiającego – 1 szt.:

Producent	
Typ/model	
Numer produktu	

Charakterystyka (wymagania minimalne)	Spełnia tak/nie
1. Zapora sieciowa typu Next Generation Firewall (NGFW). 2. Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku. 3. Minimalna ilość interfejsów: 1) 2 interfejsów 1G SFP, 2) 8 interfejsy RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa, 3) 1 interfejs konsoli Micro-USB do zarządzania zaporą, 4) 1 interfejs USB typ-C, do podłączenia modemu 5G/LTE 4. Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa. 5. Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji. 6. Możliwość utworzenia przynajmniej 64 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q. 7. Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej. 8. Minimalna ilość jednocześnie obsługiwanych połączeń: 1 000 000. 9. Możliwość obsłużenia przynajmniej 12 000 nowych połączeń w ciągu 1 sekundy. 10. Przepustowość urządzenia pracującego w trybie stateful firewall: 2,5 Gbps – dla ramki 1518B zgodnie z RFC 2544. 11. Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 1.5 Gbps. 12. Przepustowość urządzenia pracującego jako koncentrator VPN: 1,2 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544. 13. Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) – 1 Gbps. 14. Minimalna ilość jednocześnie zestawionych tuneli sitesite VPN (urządzenie – urządzenie): 200. 15. Minimalna ilość licencji umożliwiających zestawienie połączeń clientsite SSL VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 1 z możliwością rozszerzenia do przynajmniej 50. 16. Minimalna ilość licencji umożliwiających zestawienie połączeń clientsite IPsec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 5 z możliwością rozszerzenia do przynajmniej 200. 17. Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do	

inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne. 18. Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 430 Mbps oraz obsługiwać 35 000 połączeń. 19. Obsługa IPsec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP, AESGCM16-256. 20. Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie sitesite oraz clientsite). 21. Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa). 22. Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP, SAML. 23. Wsparcie dla Dynamicznego DNS tzw. DDNS. 24. Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne. 25. Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio). 26. Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak: 1) wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron), 2) wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony, 3) wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki. 27. Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps. 28. Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL. 29. Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bez-przewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPsec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci. 30. Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje LoadBalancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego. 31. Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN). 32. Kontrola dostępności zestawionych tuneli VPN. 33. Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP. 34. Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty.	
--	--

35. Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić).
36. Funkcja NAT oparta o reguły bezpieczeństwa.
37. NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe).
38. Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych.
39. Zintegrowany system skanowania antyspyware.
40. Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www.
41. Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (re-gex).
42. Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji:
 - 1) Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie.
 - 2) Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur.
 - 3) Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur.
43. System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików.
44. Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa.
45. Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi.
46. Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p.
47. Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń.
48. Rozwiązanie weryfikuje użyte na urządzeniu hasła lokalne, LDAP bind passwords i inne credentials (w tym używane przez userów LDAP) pod kątem wycieków i słabości, porównując z bazą compromised passwords i powiadamia o problemach lub blokuje do-stęp dla haseł skompromitowanych.
49. Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 4 silników pochodzących od różnych producentów w ce-lu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach. Funkcjonalność nie może wymagać zakupu dodatkowych licencji.
50. Urządzenie powinno posiadać możliwość realizacji funkcjonalności SD-WAN bazując minimum na poniższych parametrach: Jitter, Latency, Packet Loss. Funkcjonalność nie może wymagać zakupu dodatkowych licencji.
51. Urządzenie powinno posiadać zintegrowany kontroler sieci bez-przewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do 16 takich punktów dostępowych sieci bezprzewodowej.

Znak sprawy: ZP.2.2026

„Dostawa sprzętu informatycznego w ramach realizacji projektu – CyberKropla – Cyberbezpieczny Wodociąg w Darłowie”

52. Urządzenie dostarczone z elementami niezbędnymi do zamocowania w szafie RACK 19". Wszystkie wymagane do tego elementy muszą pochodzić od tego samego producenta	
Gwarancja: Min. 12 mc, wsparcie w trybie 24x7.	
Wymagane licencje: 1) Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 1 rok. 2) Licencja na centralne zarządzanie DNS z funkcjami takimi jak filtrowanie zapytań DNS. Usługa bazując na 19 predefiniowanych kategoriach, umożliwia utworzenie polityk pozwalających podjęcie 4 działań w oparciu o skonfigurowane profile. Licencje ważne 1 rok. 3) Licencja na usługę przechowywania logów z systemu firewall i generowania na ich podstawie raportów oraz oprogramowanie do zarządzania systemami firewall. Obydwie funkcjonalności muszą być obsługiwane z tej samej konsoli. Dane przechowywane są poza infrastrukturą klienta na terenie Unii Europejskiej. Licencja powinna umożliwiać przechowywanie logów przez okres minimum 7 dni. Eksport danych z zapory sieciowej powinien odbywać się za pomocą protokołu IPFIX. W celach zapewnienia kompatybilności oprogramowanie powinno pochodzić od tego samego producenta co system firewall. Wymagana jest licencja, która pozwoli na korzystanie z oprogramowania przez okres 1 rok. System do zarządzania powinien umożliwiać m.in.: wykonywania szablonów konfiguracyjnych i zarządzania nimi, ob-sługiwać funkcjonalność „zerotouch”, tworzenia sieci VPN oraz konfiguracji SD-WAN za pomocą kreatora, zastosowania konfiguracji o wybranej porze dnia, znajdowania różnic pomiędzy konfiguracją zapisaną na urządzeniu a nową tworzoną przez administratora.	

UTM do oczyszczalni ścieków w Rusku – 1 szt.:

Producent	
Typ/model	
Numer produktu	

Charakterystyka (wymagania minimalne)	Spełnia tak/nie
1. Zapora sieciowa typu Next Generation Firewall (NGFW). 2. Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku. 3. Minimalna ilość interfejsów: 1) 1 interfejs 1G SFP, 2) 4 interfejsy RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa, 3) 1 interfejs konsoli Micro-USB do zarządzania zaporą, 4) 1 interfejs USB typ-C, do podłączenia modemu 5G/LTE. 4. Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa. 5. Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji. 6. Możliwość utworzenia przynajmniej 64 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q. 7. Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej. 8. Minimalna ilość jednocześnie obsługiwanych połączeń: 300 000.	

9. Możliwość obsłużenia przynajmniej 7 500 nowych połączeń w ciągu 1 sekundy.
10. Przepustowość urządzenia pracującego w trybie stateful firewall: 0,75 Gbps – dla ramki 1518B zgodnie z RFC 2544.
11. Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 0.75 Gbps.
12. Przepustowość urządzenia pracującego jako koncentrator VPN: 0,75 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544.
13. Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń, jeśli chodzi o wielkość skanowanych plików) – 750 Mbps.
14. Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 50.
15. Minimalna ilość licencji umożliwiających zestawienie połączeń clientsite SSL VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 1 z możliwością rozszerzenia do przynajmniej 5.
16. Minimalna ilość licencji umożliwiających zestawienie połączeń clientsite IPsec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 1 z możliwością rozszerzenia do przynajmniej 5.
17. Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne.
18. Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 250 Mbps oraz obsłużyć 10 000 połączeń.
19. Obsługa IPsec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP, AESGCM16-256.
20. Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site).
21. Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa).
22. Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP, SAML.
23. Wsparcie dla Dynamicznego DNS tzw. DDNS.
24. Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne.
25. Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony, na które użytkownik wchodzi bezpośrednio).
26. Administrator powinien mieć możliwość tworzenia różnych akcji, dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:
 - 1) wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron),
 - 2) wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony,
 - 3) wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki.
27. Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps.
28. Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL.

29. Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci.
30. Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego.
31. Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN).
32. Kontrola dostępności zestawionych tuneli VPN.
33. Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP.
34. Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty.
35. Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić).
36. Funkcja NAT oparta o reguły bezpieczeństwa.
37. NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe).
38. Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych.
39. Zintegrowany system skanowania antyspyware,.
40. Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www.
41. Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex).
42. Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji.
 - 1) Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie.
 - 2) Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur.
 - 3) Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur.
43. System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików.
44. Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa.
45. Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi.
46. Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja

Znak sprawy: ZP.2.2026

„Dostawa sprzętu informatycznego w ramach realizacji projektu – CyberKropla – Cyberbezpieczny Wodociąg w Darłowie”

pasma, DSCP, 802.1p. 47. Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń. 48. Rozwiązanie weryfikuje użyte na urządzeniu hasła lokalne, LDAP bind passwords i inne credentials (w tym używane przez userów LDAP) pod kątem wycieków i słabości, porównując z bazą compromised passwords i powiadamia o problemach lub blokuje dostęp dla haseł skompromitowanych. 49. Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 4 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach. Funkcjonalność nie może wymagać zakupu dodatkowych licencji. 50. Urządzenie powinno posiadać możliwość realizacji funkcjonalności SD-WAN bazując minimum na poniższych parametrach: Jitter, Latency, Packet Loss. Funkcjonalność nie może wymagać zakupu dodatkowych licencji. 51. Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do 2 takich punktów dostępowych sieci bezprzewodowej.	
Gwarancja: Min. 12 mc, wsparcie w trybie 24x7.	
Wymagane licencje: 1) Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 1 roku. 2) Licencja na centralne zarządzanie DNS z funkcjami takimi jak filtrowanie zapytań DNS. Usługa bazując na 19 predefiniowanych kategoriach, umożliwia utworzenie polityk pozwalających podjęcie 4 działań w oparciu o skonfigurowane profile. Licencje ważne 1 rok. 3) Licencja na usługę przechowywania logów z systemu firewall i generowania na ich podstawie raportów oraz oprogramowanie do zarządzania systemami firewall. Obydwie funkcjonalności muszą być obsługiwane z tej samej konsoli. Dane przechowywane są poza infrastrukturą klienta na terenie Unii Europejskiej. Licencja powinna umożliwiać przechowywanie logów przez okres minimum 7 dni. Eksport danych z zapory sieciowej powinien odbywać się za pomocą protokołu IPFIX. W celach zapewnienia kompatybilności oprogramowanie powinno pochodzić od tego samego producenta co system firewall. Wymagana jest licencja, która pozwoli na korzystanie z oprogramowania przez okres 1 roku. System do zarządzania powinien umożliwiać m.in.: wykonywania szablonów konfiguracyjnych i zarządzania nimi, obsługiwać funkcjonalność „zerotouch”, tworzenia sieci VPN oraz konfiguracji SD-WAN za pomocą kreatora, zastosowania konfiguracji o wybranej porze dnia, znajdowania różnic pomiędzy konfiguracją zapisaną na urządzeniu a nową tworzoną przez administratora.	

MINIMALNE WYMAGANIA TECHNICZNO – UŻYTKOWE

Część nr 5 – Dostawa Access Point Wi-Fi z centralnym zarządzaniem

Access Point Wi-Fi z centralnym zarządzaniem – 2 szt.:

Producent	
Typ/model	
Numer produktu	

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie
Typ	Bezprzewodowy punkt dostępowy klasy enterprise, do pracy wewnątrz budynków	
Standard	IEEE 802.11a/b/g/n/ac/ax/be (Wi-Fi 7)	
Pasma	Jednoczesna obsługa 2,4 GHz, 5 GHz i 6 GHz	
MIMO	Minimum 2×2 MIMO dla każdego pasma	
Wi-Fi 7	Obsługa MLO, OFDMA, MU-MIMO, 4096-QAM	
Kanał radiowy	Szerokość kanału do 320 MHz	
Prędkość	Łączna przepustowość radiowa minimum 8 Gb/s	
Porty LAN	Minimum 2 × RJ-45 100/1000/2500/5000 Mb/s	
PoE	IEEE 802.3bt PoE++	
VLAN	IEEE 802.1Q, możliwość przypisania VLAN do SSID	
SSID	Minimum 8 niezależnych SSID	
Bezpieczeństwo	WPA2/WPA3 Personal i Enterprise, 802.1X, RADIUS	
Roaming	Obsługa 802.11k, 802.11v i 802.11r	
Zarządzanie radiowe	Automatyczny dobór kanału i mocy nadajnika	
Zarządzanie	Web GUI, CLI, SNMP, centralne zarządzanie wieloma AP	
Monitoring	Monitoring klientów, parametrów radiowych i zdarzeń oraz możliwość eksportu logów	
IPv4/IPv6	Wymagana obsługa	
Montaż	Montaż ścienny lub sufitowy, uchwyt montażowy w zestawie	
Praca	24/7	
Temperatura pracy	Co najmniej 0–50°C	
Gwarancja	Minimum 36 miesięcy	

MINIMALNE WYMAGANIA TECHNICZNO – UŻYTKOWE

Część nr 6 – Dostawa zasilacza awaryjnego (UPS)

Zasilacz awaryjny – 1 szt.:

Producent	
Typ/model	
Numer produktu	

Parametr	Charakterystyka (wymagania minimalne)	Spełnia tak/nie
Typ	Bezprzerwowy zasilacz UPS o mocy 3000VA /2700 który musi zapewnić czas podtrzymania minimum 9 minut dla obciążenia 2000 W. Zasilacz UPS wykonany w architekturze line interactive.	
Parametry wejściowe	- Napięcie: 230 V (1-fazowe), tolerancja 166 - 278V AC bez zmniejszenia mocy - Częstotliwość: 50/60 Hz, tolerancja 45-65 Hz - Ochrona przeciwudarowa: 624J (624J L/N, 624J L/G, 624J N/G) - Gniazdo C20, bezpiecznik automatyczny 16A - Elektroniczne zabezpieczenie przed przetężeniem, przeciwzwarciove z wyłączeniem	
Parametry wyjściowe	- Napięcie (czysty przebieg sinusoidalny): 230V - Częstotliwość: 50 Hz - Współczynnik mocy 0,9 - Przebieżalność w trybie pracy normalnej: 106% – 125% przez 60 s 126%–150% przez 50 s 151% – 200% przez 2 s - Przebieżalność falownika w trybie baterijnym: 111% – 120% przez 10 s; powyżej 121% – wyłączenie - Czas przełączania 4 – 6ms typowo (regulowana czułość) - Czysta sinusoida w trybie baterijnym - Sprawność w trybie regulacji napięcia (buck, boost) 96%, 98% bez regulacji napięcia - Ilość gniazd: (3) IEC 320 C13, (1) IEC 320 C19 + grupa gniazd sterowanych (3) IEC 320 C13 - UPS powinien móc się wyłączyć po 3h jeśli obciążenie na wyjściu wynosi mniej niż 5%/10%/15% z możliwością wyłączenia tej funkcji.	
Bateria	6x9Ahx12V AGM VRLA 3-5letnia - muszą zapewnić czas podtrzymania minimum 9 minut dla obciążenia 2000W. - Hot-swap - Czas ładowania baterii wewnętrznej do 90%: 4h (typowo) przy pełnym obciążeniu, po całkowitym wyładowaniu. - Automatyczny test co 8 tygodni (konfigurowalne), przy uruchomieniu i na żądanie użytkownika. - Obsługa do 6 modułów bateryjnych	

Znak sprawy: ZP.2.2026

„Dostawa sprzętu informatycznego w ramach realizacji projektu – CyberKropla – Cyberbezpieczny Wodociąg w Darłowie”

Zgodność z normami	• Bezpieczeństwo: IEC/EN62040-1:2008+A1:2013 • Certyfikaty: CE, CB Report, ISTA2A • Środowiskowe: RoHS2 / REACH / WEEE	
Parametry środowiskowe	• Temperatura pracy od 0 °C do +40 °C • Wilgotność: 8-90 % bez kondensacji • Głośność: <40db w trybie normalnym przy mniej niż 70% obciążenia, <45dB w trybie regulacji napięcia powyżej 70% obciążenia, < 55dBA w trybie bateryjnym	
Gabaryty	Wymiary zasilacza UPS nie mogą być większe niż: szer. x głęb. x wys. (mm) 438 x 630 x 88 Waga: 32kg	
Sterowanie zdalne, komunikacja (RDU120)	• Zasilacz UPS musi być wyposażony w kartę zarządzającą SNMP z technologią Secure Boot, certyfikowaną UL2900-1, współpracującą z systemami autoryzacji z obsługą czujników środowiskowych wykorzystujących magstrale one-wire, obsługującą systemy autoryzacji ADIUS, TACACS+ and LDAP/AD, z portem usb-C zdolną do pracy z prędkością 1Gbps. oraz wbudowany port EPO oraz gniazda USB i punkt uziemiający. • Kolorowy ciekłokrystaliczny wyświetlacz graficzny	
Gwarancja	Minimum 36 miesięcy	

(Niniejszy projekt umowy zawiera zapisy dla wszystkich części przedmiotu zamówienia, ale ostatecznie umowy zostaną sporządzone osobno dla każdej z sześciu części przedmiotu zamówienia. Zamawiający kolorem czerwonym oznaczył miejsca, w których treść umowy będzie różna zależnie od tego, jaką część zamówienia będzie obejmowała.)

UMOWA Nr /2026

zawarta w dniu 2026 r. pomiędzy:

Gminnym Zakładem Użyteczności Publicznej Sp. z o. o. z siedzibą w Krupy 72, 76-150 Darłowo, NIP: 4990657295, REGON: 364588468, reprezentowanym przez Prezesa Zarządu – Tomasza Gondek (zwaną dalej „Zamawiającym”),

a

.....
z siedzibą w, NIP
reprezentowanym przez
(zwanym dalej „Wykonawcą”),

w wyniku postępowania o udzielenie zamówienia publicznego przeprowadzonego w trybie podstawowym na podstawie art. 275 pkt. 1 została zawarta umowa o następującej treści:

§ 1

1. Przedmiotem zamówienia jest dostawa sprzętu informatycznego w ramach realizacji projektu – CyberKropla – Cyberbezpieczny Wodociąg w Darłowie – część nr
2. Zamówienie współfinansowane jest w ramach Krajowego Planu Odbudowy i Zwiększania Odporności, Działanie C3.1.1 Cyberbezpieczeństwo – CyberPL. Konkurs grantowy o numerze KPOD.05.10-CW.01-001/25.

§ 2

(Umowy sporządzone zostaną osobno dla każdej z sześciu części przedmiotu zamówienia, a ostateczna treść § 2 umowy dotyczyła będzie wyłącznie części, na którą złożona została oferta Wykonawcy.)

Część nr 1:

1. Szczegółowy opis sprzętu informatycznego znajduje się w załączniku nr 2a do SWZ.
2. Przedmiot dostawy powinien zostać dostarczony do siedziby Zamawiającego.

Część nr 2:

1. Szczegółowy opis sprzętu informatycznego znajduje się w załączniku nr 2b do SWZ.
2. Przedmiot dostawy powinien zostać dostarczony do siedziby Zamawiającego.

Część nr 3:

1. Szczegółowy opis sprzętu informatycznego znajduje się w załączniku nr 2c do SWZ.
2. Przedmiot dostawy powinien zostać dostarczony do siedziby Zamawiającego.

Część nr 4:

1. Szczegółowy opis sprzętu informatycznego znajduje się w załączniku nr 2d do SWZ.

Znak sprawy: ZP.2.2026

„Dostawa sprzętu informatycznego w ramach realizacji projektu – CyberKropla – Cyberbezpieczny Wodociąg w Darłowie”

2. Przedmiot dostawy powinien zostać dostarczony do siedziby Zamawiającego oraz oczyszczalni ścieków w Rusku.

Część nr 5:

1. Szczegółowy opis sprzętu informatycznego znajduje się w załączniku nr 2e do SWZ.
2. Przedmiot dostawy powinien zostać dostarczony do siedziby Zamawiającego.

Część nr 6:

1. Szczegółowy opis sprzętu informatycznego znajduje się w załączniku nr 2f do SWZ.
2. Przedmiot dostawy powinien zostać dostarczony do siedziby Zamawiającego.

3. Wymagania ogólne:

- 6) O ile inaczej nie zaznaczono, wszelkie zapisy SWZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.
- 7) Dostarczany sprzęt musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w styczniu 2025 r., wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie, pochodzić z oficjalnego kanału dystrybucyjnego. Przez stwierdzenie „fabrycznie nowy” należy rozumieć sprzęt opakowany oryginalnie (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Przez „wadę fizyczną” należy rozumieć również jakąkolwiek niezgodność ze opisem przedmiotu zamówienia.
- 8) Sprzęt musi być wyposażony we wszystkie niezbędne do jego działania i zapewnienia wymaganych funkcjonalności Sprzętu standardowe rozwiązania software’owe wraz z prawem do bezterminowego korzystania przez Zamawiającego z tych rozwiązań w takiej funkcji, jednakże w każdym przypadku nie krócej, niż przez czas, w jakim będzie technicznie możliwe używanie Sprzętu.
- 9) Dokumenty gwarancyjne wystawiane i przekazywane przez Wykonawcę powinny być zgodne z zapisami SWZ.
- 10) Oprogramowanie pochodzić będzie z legalnego, tj. akceptowanego przez producenta Oprogramowania kanału dystrybucji oraz zostanie udostępnione Zamawiającemu do korzystania na warunkach stosowanych lub akceptowanych przez takiego producenta.

4. Kryteria równoważności:

- 4) W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.
- 5) W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm polskich lub europejskich, ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 5 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.
- 6) Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w

SWZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.

§ 3

Wykonawca dostarczy przedmiot zamówienia w terminie 60 dni od dnia podpisania umowy.

§ 4

1. Za wykonanie przedmiotu umowy określonego w § 1 i 2 wynagrodzenie ustalone na podstawie oferty wynosi:
 - 1) Wartość netto: zł,
 - 2) VAT – %: zł,
 - 3) **Wartość brutto: zł,**
 - 4) Słownie:
2. Wynagrodzenie określone w ust. 1 niniejszego paragrafu, obejmuje całość kosztów związanych z realizacją przedmiotu umowy i nie podlega zmianie w trakcie jej wykonywania.
3. Wykonawcy poza kwotą wynagrodzenia, określoną w ust. 1 niniejszego paragrafu, nie przysługują żadne roszczenia majątkowe wobec Zamawiającego z tytułu wykonania przedmiotu umowy.
4. Wynagrodzenie będzie wypłacone po wykonaniu całości przedmiotu zamówienia.
5. Termin płatności wynosi dni od dnia otrzymania prawidłowo wystawionej faktury.
6. Forma płatności: przelew na konto bankowe Wykonawcy wskazane na fakturze. Rachunek bankowy Wykonawcy musi być zgodny z numerem rachunku ujawnionym w wykazie podmiotów zarejestrowanych jako podatnicy VAT, niezarejestrowanych oraz wykreślonych i przywróconych do rejestru VAT, prowadzonym przez Szefa Krajowej Administracji Skarbowej, zwanym dalej „wykazem”. Gdy w wykazie ujawniony będzie inny rachunek bankowy, płatność wynagrodzenia dokonana zostanie na rachunek bankowy ujawniony w wykazie. W przypadku, gdy Wykonawca nie figuruje w wykazie zobowiązany jest ujawnić swój numer rachunku bankowego w wykazie. Zamawiający wstrzyma do czasu ustania przyczyny płatność faktury w przypadku niewywiązania się Wykonawcy z zobowiązania ujawnienia rachunku bankowego w wykazie. Wstrzymanie wypłaty wynagrodzenia nie rodzi w tych przypadkach po stronie Zamawiającego opóźnienia i Wykonawcy nie przysługują odsetki z tego tytułu.
7. W przypadku nieterminowej płatności Wykonawcy za opóźnienie przysługują odsetki ustawowe

§ 5

1. Wykonawca zobowiązany jest do wykonania przedmiotu umowy zgodnie z postanowieniami SWZ, przepisami prawa i obowiązującymi w tym zakresie normami technicznymi.
2. Wykonawca, który powołuje się na rozwiązania równoważne opisane przez Zamawiającego, jest zobowiązany wykazać, że oferowane przez niego dostawy, spełniają wymagania określone przez Zamawiającego. Obowiązek Wykonawcy wykazania równoważności produktu jest obowiązkiem wynikającym z ustawy, który może być spełniony w jakikolwiek sposób pozwalający Zamawiającemu jednoznacznie stwierdzić zgodność oferowanych w ofercie produktów z wymaganiami określonymi w SWZ.

§ 6

1. Jeżeli w toku czynności odbioru zostaną stwierdzone wady Zamawiający ma prawo do:

- 1) jeżeli wady nadają się do usunięcia – odmowy odbioru przedmiotu umowy do czasu usunięcia wad, wyznaczając termin na ich usunięcie,
- 2) jeżeli wady nie nadają się do usunięcia, to:
 - a) gdy wady umożliwiają prawidłowe użytkowanie przedmiotu dostawy zgodnie z przeznaczeniem – Zamawiający może żądać obniżenia odpowiednio wynagrodzenia Wykonawcy,
 - b) gdy wady uniemożliwiają prawidłowe użytkowanie przedmiotu dostawy zgodnie z przeznaczeniem – Zamawiający może odstąpić od umowy lub żądać dostawy nowego przedmiotu umowy.
2. Wykonawca jest zobowiązany do pisemnego zawiadomienia Zamawiającego o usunięciu wad oraz do żądania wyznaczenia terminu do odbioru zakwestionowanego przedmiotu dostawy.
3. W przypadku opóźnienia w terminie usunięcia wad stwierdzonych podczas odbioru Zamawiający naliczy Wykonawcy kary umowne, o których mowa w § 7 ust. 1 pkt. 2 umowy.
4. Jeżeli w ramach gwarancji jakości, Wykonawca usunął wadę istotną, gwarancji biegnie na nowo od chwili usunięcia wady. W pozostałych przypadkach termin gwarancji ulega przedłużeniu o czas, w którym wada była usuwana. Zarzut z tytułu gwarancji jakości Zamawiający może podnieść po upływie terminów określonych w niniejszym paragrafie, jeżeli przed ich upływem zawiadomił Wykonawcę o wadzie.

§ 7

1. Strony ustalają, że Wykonawca zapłaci Zamawiającemu kary umowne z następujących tytułów:
 - 1) za zwłokę w wydaniu przedmiotu umowy w wysokości 0,2% kwoty wynagrodzenia brutto określonego w § 4 ust. 1 pkt. 3 za każdy dzień zwłoki;
 - 2) za zwłokę w usunięciu braków, wad lub usterek stwierdzonych przy odbiorze lub w okresie rękojmi za wady w wysokości 0,2% kwoty wynagrodzenia brutto określonego w § 4 ust. 1 pkt. 3 za każdy dzień zwłoki liczony od dnia wyznaczonego na usunięcie wad;
 - 3) za odstąpienie przez Zamawiającego od umowy z powodu okoliczności, za które odpowiada Wykonawca w wysokości 10% kwoty wynagrodzenia brutto określonego w § 4 ust. 1 pkt. 3;
 - 4) za odstąpienie przez Wykonawcę od umowy z powodu okoliczności, za które odpowiada on sam w wysokości 10% kwoty wynagrodzenia brutto określonego w § 4 ust. 1 pkt. 3.
2. Łączna wysokość kar umownych naliczonych Wykonawcy przez Zamawiającego nie może przekroczyć 20 % kwoty wynagrodzenia brutto określonego w § 4 ust. 1 pkt. 3.
3. Zamawiający zastrzega sobie, a Wykonawca wyraża zgodę, na potrącenie należności wynikających z kar umownych z przysługującego Wykonawcy wynagrodzenia za wykonanie przedmiotu umowy.
4. Postanowienia ust. 1 nie wyłączają prawa Zamawiającego do dochodzenia od Wykonawcy odszkodowania uzupełniającego na zasadach ogólnych, jeżeli wartość powstałej szkody przekroczy wysokość kar umownych.
5. W razie zaistnienia istotnej zamiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o tych okolicznościach. W takim przypadku Wykonawca może żądać jedynie wynagrodzenia należnego mu z tytułu wykonania części umowy.

§ 8

1. Zamawiający przewiduje możliwość dokonania zmiany postanowień umowy na podstawie art. 455 ustawy Prawo zamówień publicznych, które zostaną wyrażone w formie pisemnego aneksu pod rygorem nieważności i mogą nastąpić wyłącznie w następujących sytuacjach:
 - 1) zmiany terminu wykonania umowy, w przypadku:
 - a) wystąpienia okoliczności, których nie można było przewidzieć w chwili zawarcia umowy,
 - b) wstrzymanie realizacji przedmiotu umowy przez Zamawiającego nie wynikające z przyczyn leżących po stronie Wykonawcy,
 - c) wyrażenia zgody przez Zamawiającego na skrócenie terminu realizacji,
 - 3) w zakresie zmiany wynagrodzenia, zwłaszcza w sytuacji zmiany stawki obowiązującego podatku od towarów i usług (VAT).
2. Warunkiem dokonania zmian, o których mowa w ust. 1, jest złożenie wniosku przez stronę inicjującą zmianę zawierającego:
 - 1) opis propozycji zmiany,
 - 2) uzasadnienie zmiany,
 - 3) obliczenie kosztów zmiany zgodnie z zasadami określonymi w umowie, jeżeli zmiana będzie miała wpływ na wynagrodzenie Wykonawcy,
 - 4) opis wpływu zmiany na harmonogram realizacji i fakturowania oraz termin wykonania umowy.
3. Wykonawca nie będzie uprawniony do żądania przedłużenia terminu wykonania umowy i zwiększenia wynagrodzenia, jeżeli zmiana jest wymuszona uchybieniem czy naruszeniem umowy przez Wykonawcę – w takim przypadku koszty dodatkowe związane takimi zmianami ponosi Wykonawca.
4. Powyższe zmiany nie mogą być niekorzystne dla Zamawiającego.
5. Poza przypadkami opisanymi w niniejszym paragrafie, zmiana umowy może nastąpić w przypadkach przewidzianych w art. 455 ust. 1 pkt. 2 – 4 i ust. 2 ustawy Prawo zamówień publicznych.

§ 9

1. Za W kwestiach nieuregulowanych niniejszą umową mają zastosowanie postanowienia ustawy Prawo zamówień publicznych i Kodeksu Cywilnego.
2. Ewentualne spory wynikłe w związku z realizacją umowy będą rozstrzygane przez sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
3. Niniejszą umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.
4. Integralnymi częściami niniejszej umowy są:
 - 1) Oferta Wykonawcy.
 - 2) SWZ.

ZAMAWIAJĄCY:**WYKONAWCA:**

Nazwa wykonawcy

Adres wykonawcy

O Ś W I A D C Z E N I E

Na potrzeby postępowania o udzielenie zamówienia publicznego, pn. **„Dostawa sprzętu informatycznego w ramach realizacji projektu – CyberKropla – Cyberbezpieczny Wodociąg w Darłowie”** prowadzonego przez Gminny Zakład Użyteczności Publicznej Sp. z o. o. oświadczam, co następuje:

1. nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust 1 ustawy Pzp;
2. nie podlegam wykluczeniu z postępowania na podstawie art. 109 ust. 1 ustawy Pzp;
3. nie podlegam wykluczeniu z postępowania na podstawie art. 7 ust 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t.j. Dz. U. z 2025, poz. 514 z późn. zm.);
4. *zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ustawy Pzp (podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2, 5 i 6 lub art. 109 ust. 1 pkt. 2-10 ustawy Pzp). Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjąłem następujące środki naprawcze:
.....
.....
.....
.....
5. *następujący/e podmiot/y, na którego/ych zasoby powołuję się w niniejszym postępowaniu, tj.:
.....
.....
.....
.....
nie podlega/ją wykluczeniu z postępowania o udzielenie zamówienia;
6. *następujący/e podmiot/y, będący/e podwykonawcą/ami:
.....
.....
.....
.....
nie podlega/ą wykluczeniu z postępowania o udzielenie zamówienia;

7. spełniam warunki udziału w postępowaniu określone przez zamawiającego w specyfikacji warunków zamówienia.
8. *w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w specyfikacji warunków zamówienia, polegam na zasobach następującego/ych podmiotu/ów:
.....
.....
.....
.....
w następującym zakresie:
.....
.....
.....
.....
9. wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.
10. zapoznaliśmy się z warunkami realizacji zamówienia publicznego oraz przyjmujemy je do realizacji bez zastrzeżeń.
11. zapoznaliśmy się ze specyfikacją warunków zamówienia, nie wnosimy do niej uwag ani zastrzeżeń
12. zapoznaliśmy się z formularzem projektu umowy (**Załącznik nr 3 do SWZ**) i nie wnosimy do niego zastrzeżeń.
13. zdobyliśmy wszelkie możliwe informacje w celu należytego przygotowania oferty, w tym określenia ceny naszej oferty.
14. udzielimy wszelkich możliwych wyjaśnień dotyczących złożonej przez nas oferty.

.....
Podpis wykonawcy

Miejscowość i data:

**niepotrzebne skreślić*

Oświadczenia wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 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. U. UE L z 2016 r. Nr 119 poz. 1 i z 2018 r. Nr 127 poz. 2) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

.....
Podpis wykonawcy

Miejscowość i data: