Cyberbezpieczne Wodociągi

ZAMAWIAJĄCY:

Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o.
ul. Graniczna 1
05-200 Wołomin

Przetarg nieograniczony na:

„Opracowanie dokumentacji i wykonanie audytów – obszar organizacyjny w ramach projektu „Cyberbezpieczne Wodociągi" realizowanego przez Przedsiębiorstwo Wodociągów i Kanalizacji Sp.z o.o. w Wołominie, w ramach Inwestycji C3.1.1 „Cyberbezpieczeństwo – CyberPL" – Cyberbezpieczne Wodociągi, finansowanego z Krajowego Planu Odbudowy i Zwiększania Odporności"

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA (SWZ)

Nr DI/12/2026

Zatwierdził

.....

Dokument podpisany przez Wojciech Jankowski
Data: 2026.07.24 09:26:20 CEST

PREZES ZARZĄDU
Wojciech Jankowski

Wołomin, lipiec 2026

4

KRAJOWY PLAN ODBUDOWY | Rzeczpospolita Polska | Sfinansowane przez Unię Europejską NextGenerationEU

Spis treści

Cyberbezpieczne Wodociągi

INFORMACJE OGÓLNE

Zamawiający:
Przedsiębiorstwo Wodociągów i Kanalizacji Spółka z o.o.
ul. Graniczna 1, 05-200 Wołomin
tel. (022) 776-21-21
NIP 125-00-05-499
e-mail: pwik@pwik.wolomin.pl

Tryb udzielenia zamówienia:

Postępowanie na zamówienie w trybie przetargu nieograniczonego prowadzone na podstawie „Regulaminu udzielania przez Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o. z siedzibą w Wołominie zamówień nieobjętych ustawą z dnia 11 września 2019 r. Prawo Zamówień Publicznych" – zatwierdzonego Uchwałą nr 4/2026 z dnia 23.02.2026 r.

- Wszelkie koszty związane z przygotowaniem i złożeniem oferty ponosi Oferent.
- Oferent winien zapoznać się z całością niniejszej SWZ wraz z załącznikami do niej.
- Wszystkie dodatki stanowią integralną część SWZ.
- Zamawiający nie dopuszcza składania ofert częściowych
- Zamawiający nie dopuszcza składania ofert wariantowych
- Zamawiający nie przewiduje udzielania zamówień uzupełniających.
- Rozliczenia między Zamawiającym a Wykonawcą prowadzone będą w PLN.
- Oferta musi być zabezpieczona wadium w wysokości: 3 000,00 zł
- SWZ dostępna na stronie Zamawiającego www.pwik.wolomin.pl oraz na stronie https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/
- Zamawiający informuje, iż w prowadzonym przez niego przedsiębiorstwie obowiązuje procedura zgłoszeń wewnętrznych w rozumieniu ustawy z dnia 14.06.2024 r. o ochronie sygnalistów (Dz.U. z 2024 r. poz. 928 z późn. zm.), która jest dostępna na tablicy ogłoszeń w siedzibie PWIK, ul. Graniczna 1, 05-200 Wołomin.

Rozdział I
Określenie przedmiotu zamówienia

1. Przedmiotem zamówienia jest **„Opracowanie dokumentacji i wykonanie audytów – obszar organizacyjny w ramach projektu „Cyberbezpieczne Wodociągi" realizowanego przez Przedsiębiorstwo Wodociągów i Kanalizacji Sp.z o.o. w Wołominie, w ramach Inwestycji C3.1.1 „Cyberbezpieczeństwo – CyberPL" – Cyberbezpieczne Wodociągi, finansowanego z Krajowego Planu Odbudowy i Zwiększania Odporności"**
2. Szczegółowy zakres warunków zamówienia określa dodatek nr 1 do SWZ – Opis Przedmiotu Zamówienia.
3. Szczegółowe warunki realizacji zamówienia opisane są we wzorze Umowy, stanowiącej Dodatek nr 5 do SWZ.

Rozdział II
Termin realizacji

1. Wykonawca zobowiązuje się do realizacji przedmiotu zamówienia w terminie do 30.11.2026 r
2. Warunki zmiany terminu realizacji zostały określone we wzorze Umowy stanowiący Dodatek nr 5 do SWZ.

Rozdział III
Opis sposobu przygotowania Ofert

1. Ofertę stanowi druk *„OFERTA"* z załącznikami i wymaganymi dokumentami.
2. Oferent zobowiązany jest przygotować ofertę zgodnie z wymaganiami SWZ.
3. Ofertę należy złożyć w formie pisemnej.
4. W przypadku gdy informacje zawarte w ofercie stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji, co do których Wykonawca zastrzega, że nie mogą być udostępnione innym uczestnikom postępowania, muszą być one oznaczone stosowną jednoznaczną klauzulą i dołączone do oferty, zaleca się, aby były trwale oddzielone od oferty.
5. Osoby wskazane w dokumencie upoważniającym do występowania w obrocie prawnym lub posiadające pełnomocnictwo muszą złożyć podpisy na:

a) wszystkich stronach oferty;
b) załącznikach;
c) oraz w miejscach, których oferent naniósł zmiany.

6. W przypadku, gdy Oferenta reprezentuje pełnomocnik do oferty musi być załączone pełnomocnictwo z określonym zakresem, podpisane przez osoby uprawnione do reprezentowania osoby prawnej lub fizycznej.
7. W przypadku złożenia kserokopii pełnomocnictwa musi być ono potwierdzone za zgodność z oryginałem przez osoby udzielające pełnomocnictwa.
8. Wymagane dokumenty należy przedstawić w formie oryginałów albo kserokopii.
9. Dokumenty złożone w formie kserokopii muszą być opatrzone klauzulą *„ZA ZGODNOŚĆ Z ORYGINAŁEM"* i poświadczone za zgodność z oryginałem przez Oferenta w sposób umożliwiający identyfikację podpisu (np. wraz z imienną pieczątką osoby poświadczającej kopię dokumentu za zgodność z oryginałem).
10. Zamawiający zażąda przedstawienia oryginału lub notarialnie potwierdzonej kopii dokumentu wyłącznie wtedy, gdy przedstawiona przez Oferenta kserokopia dokumentu jest nieczytelna lub budzi wątpliwości, co do jej prawdziwości.
11. Oferent może zwrócić się pisemnie do Zamawiającego o wyjaśnienie do SWZ.
12. Zamawiający w ciągu 5 dni roboczych udzieli pisemnych wyjaśnień, chyba że prośba o wyjaśnienie specyfikacji wpłynęła do Zamawiającego na mniej niż 5 dni kalendarzowych przed

terminem otwarcia ofert, wówczas Zamawiający nie będzie miał obowiązku udzielenia odpowiedzi. Jednocześnie pisemna treść wyjaśnienia zostanie przesłana Oferentowi, który zadał pytanie w formie elektronicznej oraz zostanie zamieszczona na stronie internetowej oraz w siedzibie Zamawiającego.

13. W szczególnie uzasadnionych przypadkach Zamawiający może w każdym czasie, przed upływem terminu do składania ofert, zmodyfikować treść SWZ. Dokonane w ten sposób uzupełnienie stanie się częścią SWZ zaś zmieniona SWZ, dostępna będzie na stronie internetowej i w siedzibie Zamawiającego i będzie dla wszystkich Oferentów wiążąca.
14. Zamawiający przedłuża termin składania ofert lub wyznacza nowy termin przeprowadzenia przetargu, jeżeli w wyniku modyfikacji treści SWZ niezbędny jest dodatkowy czas na wprowadzenie zmian w ofertach. O przedłużeniu terminu składania ofert Zamawiający niezwłocznie zawiadamia wszystkich Oferentów, którym przekazano SWZ oraz zamieszczając informację na stronie internetowej oraz w siedzibie Zamawiającego.
15. Na wniosek Oferenta, który nie jest w stanie złożyć oferty w wyznaczonym terminie z powodu okoliczności od niego niezależnych, Zamawiający może przedłużyć termin składania ofert przed jego upływem, powiadamiając o tym wszystkich Oferentów, którzy otrzymali SWZ oraz zamieszczając informację na stronie internetowej oraz w siedzibie Zamawiającego.
16. Przedłużenie terminu składania ofert dopuszczalne jest tylko przed jego upływem.
17. Zamawiający nie zamierza zwoływać zebrania oferentów.
18. Ofertę należy sporządzić w języku polskim z zachowaniem formy pisemnej pod rygorem nieważności. W przypadku złożenia przez Wykonawcę dokumentów sporządzonych w języku obcym Zamawiający wymaga złożenia tłumaczenia na język polski.
19. Zamawiający nie dopuszcza składania ofert częściowych.
20. Oferent może złożyć tylko jedną ofertę na całe zadanie.
21. Zamawiający nie dopuszcza składania ofert wariantowych.
22. W przypadku, gdy Oferent przedłoży więcej ofert niż wskazano w pkt. 20, żadna z przedłożonych ofert nie zostanie rozpatrzona.
23. Złożona oferta musi być zgodna z Opisem przedmiotu zamówienia, który stanowi Dodatek nr 1 do SWZ.
24. **Wszystkie strony oferty muszą być kolejno ponumerowane, a oferta powinna być czytelna i trwale spięta.**
25. Każda strona oferty musi być parafowana przez osobę upoważnioną do podpisywania oferty.
26. Oferent poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.
27. Zamawiający może wykluczyć z postępowania Oferenta, na zasadach określonych w Regulaminie udzielania przez Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o. z siedzibą w Wołominie zamówień nieobjętych Ustawą z dnia 11 września 2019 r. Prawo Zamówień Publicznych – zatwierdzonego Uchwałą nr 4/2026 z dnia 23.02.2026 r.

Rozdział IV

Zmiany lub wycofanie złożonej oferty.

1. Wykonawca może wprowadzić zmiany lub wycofać złożoną przez siebie ofertę. Zmiany lub wycofanie złożonej oferty są skuteczne tylko wówczas, gdy zostały dokonane przed upływem terminu składania ofert.
2. Zmianę należy złożyć w miejscu i według zasad obowiązujących przy składaniu oferty. Odpowiednio opisaną kopertę należy opatrzyć dopiskiem „ZMIANA".
3. Wycofanie oferty następuje poprzez złożenie pisemnego powiadomienia podpisanego przez umocowanego na piśmie przedstawiciela Wykonawcy. Wycofanie należy złożyć w miejscu i według zasad obowiązujących przy składaniu oferty. Odpowiednio opisaną kopertę należy opatrzyć dopiskiem „WYCOFANIE".

Rozdział V
Sposób porozumiewania się z Wykonawcami oraz osoby uprawnione do kontaktów z Wykonawcami

1. Zamawiający zastrzega pisemną formę porozumiewania się w niniejszym postępowaniu.
2. Dopuszcza się przekazywanie drogą elektroniczną (pwik@pwik.wolomin.pl):
   - zawiadomienia o wyborze najkorzystniejszej oferty;
   - zapytań i odpowiedzi dotyczących treści SWZ;
   - informacji o zmianie treści niniejszej SWZ oraz o przedłużeniu terminu składania ofert;
   - wniosków o przekazanie SWZ,
   - wyjaśnień i uzupełnień treści złożonej oferty.
3. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o wyjaśnienia treści SWZ.
4. W przypadku rozbieżności pomiędzy treścią niniejszej SWZ a treścią udzielonych odpowiedzi jako zobowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.
5. Osobą uprawnioną do bezpośredniego kontaktowania się z Oferentami jest:
   - Sprawy techniczne – Daniel Gontarek tel. 22 776 21 21 wew. 503
   - Sprawy formalne – Urszula Papiór, tel. 22 776 21 21 wew. 515

Rozdział VI
Miejsce i sposób złożenia oferty

1. Ofertę (formularz ofertowy wraz z wymaganymi załącznikami) należy złożyć w nieprzejrzystym i zamkniętym opakowaniu.
2. Opakowanie powinno być zaadresowane na adres Zamawiającego:

   PRZEDSIĘBIORSTWO WODOCIĄGÓW I KANALIZACJI Sp. z o.o.
   ul. GRANICZNA 1, 05 – 200 WOŁOMIN

   i oznaczone hasłem:
   „Opracowanie dokumentacji i wykonanie audytów – obszar organizacyjny w ramach projektu „Cyberbezpieczne Wodociągi" realizowanego przez Przedsiębiorstwo Wodociągów i Kanalizacji Sp.z o.o. w Wołominie, w ramach Inwestycji C3.1.1 „Cyberbezpieczeństwo – CyberPL" – Cyberbezpieczne Wodociągi, finansowanego z Krajowego Planu Odbudowy i Zwiększania Odporności""
   dodatkowo na opakowaniu należy umieścić napis:
   „Nie otwierać przed terminem otwarcia ofert, tj. 07.08.2026 r. godz. 11:^{00}"
3. Na opakowaniu należy umieścić nazwę i adres Wykonawcy.
4. Zamawiający dopuszcza możliwość złożenia oferty w formie elektronicznej z podpisem kwalifikowanym na adres e-mail pwik@pwik.wolomin.pl.
5. Oferta złożona w formie elektronicznej musi być zabezpieczona hasłem, które Wykonawca prześle do Zamawiającego w dniu otwarcia ofert w godzinach od 10:45 do 11:00 na adres e-mail pwik@pwik.wolomin.pl lub sms na numer telefonu **607 314 032.**
6. **Oferta, do której Wykonawca nie prześle hasła w ww. terminie zostanie potraktowana jako niezłożona.**

Rozdział VII
Kryterium oceny Oferty

1. Zamawiający wyznaczył następujące kryteria oceny ofert i ich znaczenie:

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

L.p.	Kryteria brane pod uwagę przy ocenie ofert	Znaczenie
1.	Cena	100 %

2. O wyborze najkorzystniejszej oferty zadecyduje najniższa cena.

Rozdział VIII
Sposób obliczania ceny Oferty

1. Komisja przetargowa wybiera ofertę najkorzystniejszą spośród ofert nieodrzuconych oraz sporządzoną zgodnie ze specyfikacją warunków zamówienia.
2. Oferent zamieszcza w ofercie cenę netto oraz cenę brutto (z podatkiem VAT). Cena musi być wyrażona w złotych polskich.
3. Zamawiający oceni i porówna jedynie te oferty, które:
   - Zostaną złożone przez Wykonawców niewykluczonych przez Zamawiającego z niniejszego postępowania,
   - Nie zostaną odrzucone przez Zamawiającego.
4. Zamawiający udzieli zamówienia Wykonawcy, którego oferta będzie zawierała najniższą cenę.
5. Wszystkie ceny określone przez Wykonawcę zostaną ustalone na okres ważności umowy i nie będą podlegały zmianom. Podana w ofercie cena ryczałtowa musi uwzględniać wszystkie wymagania niniejszej SWZ oraz obejmować wszelkie koszty, jakie poniesie Wykonawca z tytułu należytej oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia, w tym musi uwzględnić ewentualne upusty i rabaty. Cena oferty będzie ostateczna i nie będzie podlegać zmianie. Oznaczać to będzie, że Wykonawca skalkuluje dodatkowo wszystkie potencjalne ryzyka, jakie mogą wystąpić przy realizacji przedmiotu umowy.
6. Cena powinna być wyrażona w PLN do dwóch miejsc po przecinku. Należy uwzględnić stawkę podatku VAT zgodną z przepisami podatkowymi – według stawki na dzień składania ofert.
7. Jeżeli nie będzie można dokonać wyboru oferty najkorzystniejszej ze względu na to, że zostały złożone oferty o takiej samej cenie, Zamawiający wezwie Wykonawców do złożenia ofert dodatkowych w określonym terminie. Wykonawcy składając oferty dodatkowe nie mogą zaoferować cen wyższych od zaoferowanych w złożonych ofertach.
8. W toku oceny ofert Zamawiający może żądać od Oferenta pisemnych wyjaśnień dotyczących treści złożonej oferty.
9. Zamawiający odrzuci ofertę, jeżeli:
   a) jest niezgodna z Regulaminem;
   b) jej treść nie odpowiada treści SWZ z zastrzeżeniem pkt. 12 lit c Rozdziału XIV SWZ;
   c) jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji;
   d) została złożona przez wykonawcę wykluczonego z udziału w postępowaniu o udzielenie zamówienia lub niezaproszonego do składania ofert;
   e) zawiera błędy w obliczeniu ceny;
   f) wykonawca w terminie 3 dni od dnia doręczenia zawiadomienia nie zgodził się na poprawienie omyłki, o której mowa w pkt. 12 lit c Rozdziału XIV SWZ;
   g) jest nieważna na podstawie odrębnych przepisów;
   h) zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia.
10. Zamawiający powiadomi o wynikach postępowania wszystkich Oferentów pisemnie, na stronie internetowej www.pwik.wolomin.pl, na stronie

https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/ oraz za pomocą ogłoszenia w siedzibie Przedsiębiorstwa.

Rozdział IX

Warunki udziału w postępowaniu o zamówienie. Informacje o dokumentach, jakie mają dostarczyć Oferenci w celu potwierdzenia spełnienia wymaganych warunków

O udzielenie zamówienia mogą ubiegać się wyłącznie Oferenci, których oferta spełnia wymagania określone w niniejszej SWZ oraz:

1. Posiadają uprawnienia do wykonywania działalności lub czynności objętych niniejszym zamówieniem, jeżeli ustawa nakłada obowiązek posiadania takich uprawnień.
2. Posiadają niezbędną wiedzę i doświadczenie.
3. Dysponują odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia.
4. Znajdują się w sytuacji ekonomicznej i finansowej umożliwiającej wykonanie przedmiotu zamówienia.

Oferent ubiegający się o zamówienie musi spełnić ww. warunki i wymagania, w celu ich potwierdzenia winien dołączyć do oferty (w formie oryginału lub kserokopii potwierdzonej za zgodność z oryginałem przez uprawomocnionego przedstawiciela Oferenta) nw. dokumenty w następującej kolejności:

a) Formularz oferty (wzór formularza oferty: *dodatek nr 2 do SWZ*) – ***załącznik nr 1***,
b) Oświadczenie Oferenta lub dokument potwierdzający, że profil działalności oferenta odpowiada przedmiotowi zamówienia oraz że Oferent jest uprawniony do występowania w obrocie prawnym, zgodnie z wymaganiami ustawowymi (aktualny odpis z właściwego rejestru albo aktualne zaświadczenie o wpisie do ewidencji działalności gospodarczej lub zgłoszenia do ewidencji działalności gospodarczej, wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert) – ***załącznik nr 2,***
c) Umowy regulujące współpracę podmiotów występujących wspólnie lub oświadczenie, że podmiot występuje samodzielnie - ***załącznik nr 3***,
d) Oświadczenie Oferenta o niekaralności w zakresie analogicznym do określonego w art. 108 i art. 109 ust. 1 pkt 4 ustawy z dnia 11 września 2019 r. Prawo Zamówień Publicznych - załącznik ***nr 4,***
e) Aktualne zaświadczenie z właściwego urzędu skarbowego o niezaleganiu oferenta z uiszczaniem podatków, wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert - ***załącznik nr 5,***
f) Aktualne zaświadczenie z właściwego oddziału Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego potwierdzającego o niezaleganiu oferenta z uiszczaniem opłat i składek, wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert – ***załącznik nr 6,***
g) Oświadczenie Oferenta, że zapoznał się ze specyfikacją warunków zamówienia oraz opisem przedmiotu zamówienia i nie wnosi do tych dokumentów zastrzeżeń, oraz uzyskał konieczne informacje i wyjaśnienia do przygotowania oferty (wzór oświadczenia: *dodatek nr 3 do SWZ*) – ***załącznik nr 7,***
h) Oświadczenie Oferenta o braku podstaw do wykluczenia z udziału w postępowaniu (wzór oświadczenia: *dodatek nr 4 do SWZ*) – ***załącznik nr 8,***
i) Parafowane wszystkie strony umowy (wzór umowy: *dodatek nr 5 do SWZ*) – ***załącznik nr 9,***
j) Upoważnienie do podpisania oferty, jeżeli ofertę podpisują inne osoby niż upoważnione do reprezentacji firmy w jej dokumentach (rejestrze lub ewidencji) (wzór upoważnienia: *dodatek nr 6 do SWZ*) – ***załącznik nr 10,***

k) Listę podmiotów należących do tej samej grupy kapitałowej, albo informację, że Wykonawca nie należy do grupy kapitałowej (*dodatek nr 7 do SWZ)* – ***załącznik nr 11,***

l) Potwierdzenie wniesienia wadium – ***załącznik nr 12,***

m) Klauzulę informacyjną – (dodatek nr 8 do SWZ) – ***załącznik nr 13,***

n) Oświadczenie Oferenta dotyczące przesłanek wykluczenia z art. 5 k Rozporządzenia 833/2014 oraz art. 7 ust. 1 Ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego - (dodatek nr 9 do SWZ) – ***załącznik nr 14,***

o) Aktualne certyfikaty potwierdzające, że jego własna organizacja funkcjonuje zgodnie z następującymi standardami zarządzania: normą ISO 9001, normą ISO/IEC 27001 oraz normą ISO 22301. Wymóg ten ma na celu zapewnienie, że podmiot odpowiedzialny za wdrażanie systemów zarządzania u Zamawiającego sam stosuje te standardy we własnej działalności. Każdy z wymaganych certyfikatów musi być wydany przez jednostkę certyfikującą akredytowaną przez Polskie Centrum Akredytacji (PCA) lub przez jednostkę akredytowaną przez organizację będącą sygnatariuszem porozumienia EA MLA (European Cooperation for Accreditation — Multilateral Agreement) lub IAF MLA (International Accreditation Forum — Multilateral Agreement). Zamawiający dopuszcza certyfikaty równoważne wystawione przez jednostki spełniające powyższe kryterium akredytacji — ciężar wykazania równoważności spoczywa na Wykonawcy. W przypadku certyfikatów równoważnych Wykonawca składa na wezwanie ponadto dokument potwierdzający akredytację jednostki certyfikującej oraz pisemne uzasadnienie równoważności. Jeżeli Wykonawca nie złoży żądanych certyfikatów lub dokumentów potwierdzających ich równoważność, są one niekompletne lub zawierają błędy, Zamawiający wezwie wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w wyznaczonym terminie. – ***załącznik nr 15 - Zamawiający przed wyborem najkorzystniejszej oferty wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie kopii wszystkich trzech certyfikatów wraz z zakresem certyfikacji i datą ważności.***

p) Wykaz, że w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał należycie:

   a) w zakresie wdrożenia systemów (SZBI lub BCP/DRP): co najmniej 2 (dwie) usługi, z których każda polegała na opracowaniu dokumentacji i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) lub opracowaniu planów ciągłości działania (BCP/DRP), o wartości nie mniejszej niż 40 000,00 zł brutto każda;

   b) w zakresie audytu: co najmniej 2 (dwie) usługi, z których każda polegała na przeprowadzeniu audytu bezpieczeństwa informacji lub audytu SZBI, o wartości nie mniejszej niż 20 000,00 zł brutto każda;

   c) w zakresie testów bezpieczeństwa: co najmniej 2 (dwie) usługi, z których każda obejmowała swoim zakresem przeprowadzenie testów penetracyjnych infrastruktury sieciowej oraz testów penetracyjnych aplikacji webowych, o wartości nie mniejszej niż 20 000,00 zł brutto każda,

   wraz z załączeniem dokumentów, referencji potwierdzających, że usługi te zostały wykonane należycie - ***załącznik nr 16,***

q) Wykaz osób, którymi Wykonawca musi dysponować na potrzeby realizacji zamówienia zespołem liczącym łącznie co najmniej 7 wykwalifikowanych osób, w skład którego wejdą specjaliści przypisani wyłącznie do jednej z trzech odrębnych grup funkcjonalnych:

   1. Zespół wdrożeniowy — SZBI, BCP/DRP, SZCD Zespół wdrożeniowy odpowiedzialny za opracowanie i wdrożenie dokumentacji SZBI, BCP/DRP oraz SZCD musi liczyć co najmniej 3 osoby zatrudnione przez Wykonawcę na podstawie umowy o pracę

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

w rozumieniu ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy. Osoby z zespołu wdrożeniowego nie mogą uczestniczyć w realizacji prac zespołu audytowego ani zespołu testów penetracyjnych. Członkowie zespołu wdrożeniowego muszą łącznie posiadać następujące kwalifikacje (dopuszcza się łączenie poniższych wymogów przez te same osoby wewnątrz tego zespołu):

a) Audytor Wiodący ds. Wdrożeń: posiada jednocześnie certyfikat Audytora Wiodącego ISO/IEC 27001 (Lead Auditor) lub równoważny, certyfikat Audytora Wiodącego ISO 22301 (Lead Auditor) lub równoważny oraz certyfikat CISA (Certified Information Systems Auditor) lub równoważny.
b) Audytor Wspomagający ds. Wdrożeń: posiada co najmniej certyfikat Audytora ISO/IEC 27001 (Auditor) lub równoważny certyfikat Audytora Wiodącego ISO 22301 (Lead Auditor) lub równoważny
c) Specjalista ds. infrastruktury i bezpieczeństwa OT/IT: posiada certyfikaty lub uprawnienia potwierdzające umiejętności w zakresie:
   i. umiejętności projektowania i wdrażania zabezpieczeń dla sieci przemysłowych (OT/ICS) (segmentacja sieci OT zgodnie z modelem Purdue, wykrywanie i profilowanie urządzeń przemysłowych, przeprowadzanie inspekcji protokołów przemysłowych (Modbus, DNP3, IEC 61850), wirtualne łatanie podatnych systemów bez przerywania ciągłości produkcji, kompetencje z zakresu centralnego monitorowania, korelacji zdarzeń bezpieczeństwa w środowiskach ICS/SCADA oraz oceny ryzyka OT
   ii. umiejętności konfiguracji i administracji firewallem nowej generacji (NGFW) – polityki bezpieczeństwa, filtrowanie ruchu, VPN (IPsec, SSL), IPS, uwierzytelnianie użytkowników i podstawowy monitoring.
   iii. znajomości sieci - potwierdzenie umiejętności w zakresie sieci komputerowych, konfiguracji i rozwiązywania problemów z urządzeniami sieciowymi (przełączniki, routery), zrozumienie modeli OSI i TCP/IP, umiejętność wdrażania routingu (OSPF, EIGRP, statyczny), konfiguracji sieci VLAN i STP, zarządzania dostępem przez ACL oraz podstawowych usługach sieciowych (DHCP, DNS, NAT), podstawy bezpieczeństwa sieci, konfiguracji VPN, zarządzania pasmem oraz wprowadzenie do automatyzacji sieci i programowalności, kompetencje w obszarze administracji i konfiguracji infrastruktury sieciowej.
   iv. uprawnień SEP E+D do 15 kV.

2. Zespół audytowy — audyty zewnętrzne SZBI, SZCD, KRI/uoKSC Zespół audytowy odpowiedzialny za przeprowadzenie audytów zewnętrznych musi liczyć co najmniej dwie osoby. Ze względu na niezależny charakter usług audytowych, Zamawiający nie wymaga zatrudnienia tych osób na podstawie umowy o pracę (dopuszczalne są formy współpracy na podstawie umów cywilnoprawnych, w tym z podwykonawcami). Osoby z zespołu audytowego nie mogą być tymi samymi osobami, które realizowały prace wdrożeniowe lub testy penetracyjne w ramach tego samego zamówienia.
   a) Pierwsza osoba (Audytor Wiodący ds. Audytów): musi posiadać jednocześnie certyfikat Audytora Wiodącego ISO/IEC 27001 (Lead Auditor) lub równoważny oraz certyfikat Audytora Wiodącego ISO 22301 (Lead Auditor) lub równoważny,
   b) Druga osoba (Audytor Wspomagający ds. Audytów): musi posiadać co najmniej certyfikat Audytora ISO/IEC 27001 (Auditor) lub równoważny.
3. Zespół testów penetracyjnych Zespół testów penetracyjnych musi liczyć co najmniej dwie osoby zatrudnione przez Wykonawcę na podstawie umowy o pracę w rozumieniu Kodeksu

pracy. Osoby z zespołu testów penetracyjnych nie mogą uczestniczyć w realizacji prac zespołu wdrożeniowego ani zespołu audytowego w ramach tego samego zamówienia.

a) Pierwsza osoba (Pentester Główny): musi posiadać jednocześnie certyfikat CEH (Certified Ethical Hacker) lub równoważny, certyfikat CISSP (Certified Information Systems Security Professional) lub równoważny oraz certyfikat eWPT (eLearnSecurity Web Application Penetration Tester) lub równoważny.
b) Druga osoba (Pentester Wspomagający): musi posiadać co najmniej certyfikat CEH lub równoważny

Zamawiający bezwzględnie zakazuje łączenia ról i funkcji pomiędzy poszczególnymi grupami funkcjonalnymi. Oznacza to, że każda osoba skierowana do realizacji zamówienia może zostać przypisana tylko do jednego zespołu. W szczególności: specjalista realizujący testy penetracyjne nie może uczestniczyć w pracach wdrożeniowych ani audytowych, a członkowie zespołu wdrożeniowego nie mogą pełnić funkcji w zespole audytowym ani penetracyjnym. Minimalny skład osobowy musi składać się z 7 odrębnych osób fizycznych.

Zamawiający wymaga zatrudnienia na podstawie stosunku pracy przez Wykonawcę osób wykonujących czynności w zakresie prac wdrożeniowych (opracowanie i wdrożenie SZBI, BCP/DRP, SZCD) oraz testów penetracyjnych infrastruktury i aplikacji.

Wymóg zatrudnienia na umowę o pracę, o którym mowa w ust. 4, nie dotyczy specjalistów realizujących audyty zewnętrzne. Ze względu na fakt, iż audytorzy mogą stanowić personel podwykonawcy, Zamawiający dopuszcza, aby osoby z zespołu audytowego realizowały swoje zadania na podstawie innych form współpracy (np. umów cywilnoprawnych, kontraktów B2B) zawartych z Wykonawcą lub podwykonawcą. – ***załącznik nr 17***

Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej zamiast dokumentów wskazanych w podpkt. b, d, e i f – składa dokument lub dokumenty wystawione w kraju, w którym ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:

- nie otwarto jego likwidacji ani nie ogłoszono upadłości – wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;
- zamiast dokumentów wskazanych w podpkt. d - składa zaświadczenie właściwego organu sądowego lub administracyjnego miejsca zamieszkania albo zamieszkania osoby, której dokumenty dotyczą, – wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

Jeżeli w miejscu zamieszkania osoby lub w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów (wskazanych w pkt. b, d, e i f), zastępuje się je dokumentem zawierającym oświadczenie złożone przed notariuszem, właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego odpowiednio miejsca zamieszkania osoby lub kraj, w którym Wykonawca ma siedzibę lub miejsce zamieszkania. Postanowienia pkt. b, d, e i f stosuje się odpowiednio.

W przypadku wątpliwości co do treści dokumentu złożonego przez Wykonawcę mającego siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, Zamawiający może zwrócić się do właściwych organów odpowiednio miejsca zamieszkania osoby lub kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, z wnioskiem o udzielenie niezbędnych informacji dotyczących przedłożonego dokumentu.

Rozdział X

Wykonawcy wspólnie ubiegający się o zamówienie

1. Wykonawcy wspólnie ubiegający się o udzielenie niniejszego zamówienia powinni pod rygorem wykluczenia z postępowania spełniać warunki udziału w postępowaniu oraz złożyć dokumenty potwierdzające spełnienie tych warunków zgodnie z zapisami zawartymi w rozdziale IX. Ponadto tacy Wykonawcy muszą ustanowić i wskazać Pełnomocnika (Lidera) do reprezentowania ich w niniejszym postępowaniu albo reprezentowania ich w postępowaniu

i zawarciu umowy w sprawie zamówienia. Zaleca się, aby Pełnomocnikiem (Liderem) był jeden z Wykonawców wspólnie ubiegających się o udzielenie zamówienia.

2. Wszelka korespondencja prowadzona będzie wyłącznie z Pełnomocnikiem (Liderem).
3. Wykonawcy wspólnie ubiegający się o udzielenie niniejszego zamówienia zobowiązani są do solidarnej odpowiedzialności za wykonanie zamówienia.
4. Wykonawcy wspólnie ubiegający się o niniejsze zamówienie, których oferta zostanie uznana za najkorzystniejszą, będą zobowiązani przedstawić Zamawiającemu stosowne porozumienie wszystkich Wykonawców składających ofertę wspólną, przed podpisaniem Umowy na realizację niniejszego zamówienia. Porozumienie takie musi zawierać w swojej treści co najmniej następujące postanowienia:
   a) określenie stron porozumienia;
   b) cel działania;
   c) okres działania na czas nie krótszy niż czas trwania odpowiedzialności Wykonawców wynikający z Umowy;
   d) sposób współdziałania (w tym rolę i zadania każdego z Wykonawców w wykonywaniu Umowy);
   e) deklarację wspólnej i solidarnej odpowiedzialności za wykonanie Umowy;
   f) wskazanie Pełnomocnika (Lidera) i jego umocowania do zaciągania zobowiązań i przyjmowania instrukcji na rzecz i w imieniu wszystkich Wykonawców razem i każdego z osobna oraz do przyjmowania płatności od Zamawiającego;
   g) deklarację niezmieniania składu ani statusu podczas całego okresu wykonywania Umowy.

   Porozumienie musi być podpisane przez upełnomocnionych przedstawicieli każdego z Wykonawców, a stosowne upoważnienia muszą wynikać z dokumentów załączonych do oferty. Pełnomocnictwo musi być złożone w formie oryginału lub poświadczonej notarialnie kopii.
5. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, dokumenty wymienione w Rozdziale IX podpkt. d, e i f każdy z tych Wykonawców składa indywidualnie.
6. Oferta powinna być podpisana w sposób wiążący prawnie wszystkich Wykonawców składających ofertę wspólną.

Rozdział XI
Korzystanie z zasobów podmiotu trzeciego

1) Wykonawca może polegać na wiedzy i doświadczeniu, osobach zdolnych do wykonania zamówienia lub zdolnościach finansowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków. Wykonawca w takiej sytuacji zobowiązany jest udowodnić Zamawiającemu, iż będzie dysponował zasobami niezbędnymi do realizacji przedmiotowego zamówienia, w szczególności przedstawiając w tym celu **pisemne zobowiązanie (w formie oryginału)** tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonywaniu przedmiotowego zamówienia.
2) Zobowiązanie podmiotu trzeciego powinno wyrażać w sposób wyraźny i jednoznaczny wolę udzielenia Wykonawcy ubiegającemu się o zamówienie odpowiedniego zasobu.
3) Jeżeli Wykonawca wykaże, że spełnia warunki udziału w postępowaniu, polegając na zasobach innych podmiotów, musi udowodnić Zamawiającemu, że będzie dysponował zasobami innych podmiotów w stopniu niezbędnym dla należytego wykonania zamówienia, oraz że stosunek łączący Wykonawcę z tymi podmiotami gwarantuje rzeczywisty dostęp do ich zasobów. Zamawiający żąda, aby z dokumentów wynikał:
   a) zakres dostępnych Wykonawcy zasobów innego podmiotu,
   b) sposób wykorzystania zasobów innego podmiotu przy wykonywaniu zamówienia,
   c) charakter stosunku, jaki będzie łączył Wykonawcę z innym podmiotem,

W przeciwnym przypadku Zamawiający wykluczy Wykonawcę z postępowania o udzielenie zamówienia.

4) Wykonawca powołujący się przy wykazaniu spełniania warunków udziału w postępowaniu na zasoby innych podmiotów, które będą brały udział w realizacji części zamówienia przedkłada także dokumenty dotyczące tego podmiotu w zakresie wymaganym dla Wykonawcy, określonym w rozdziale IX pkt. d), e) i f) SWZ.

Rozdział XII
Wadium

I. Wadium
Oferta musi być zabezpieczona wadium w wysokości 3 000,00 zł
Oferta, która nie będzie zabezpieczona określoną kwotą wadium zostanie przez Zamawiającego odrzucona.

II. Wadium może być wnoszone:
a) w pieniądzu konto Bank PKO BP SA. Na rachunek numer:
30 1020 1026 0000 1402 0262 4336
b) w poręczeniach lub w gwarancjach bankowych, gwarancjach ubezpieczeniowych złożonych u Głównego Księgowego lub w Dziale Finansowo- Księgowym w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. ul. Graniczna 1 w Wołominie

Do Oferty należy dołączyć kserokopię dokonania przelewu lub wniesienia wadium w innej formie.

1. Zamawiający dokona zwrotu wadium wszystkim Wykonawcom niezwłocznie po wyborze oferty najkorzystniejszej lub unieważnieniu postępowania, z wyjątkiem Wykonawcy, którego oferta została wybrana jako najkorzystniejsza, z zastrzeżeniem pkt 4a.

1a. Wykonawcy, którego oferta została wybrana jako najkorzystniejsza, Zamawiający zwraca wadium, niezwłocznie po zawarciu umowy zamówienia publicznego oraz wniesieniu zabezpieczenia należytego wykonania umowy.

2. Zamawiający zwraca niezwłocznie wadium na wniosek Wykonawcy, który wycofał ofertę przed upływem terminu składania ofert.

3. Zamawiający żąda ponownego wniesienia wadium przez Wykonawcę, któremu zwrócono wadium na podstawie ust. 1, jeżeli w wyniku rozstrzygnięcia odwołania jego oferta została wybrana jako najkorzystniejsza. Wykonawca wnosi wadium w terminie określonym przez Zamawiającego.

4. Jeżeli wadium wniesiono w pieniądzu, Zamawiający zwraca je wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszty prowadzenia rachunku bankowego oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy wskazany przez Wykonawcę.

4a. Zamawiający zatrzymuje wadium wraz z odsetkami, jeżeli Wykonawca w odpowiedzi na wezwanie, nie złożył wymaganych dokumentów lub oświadczeń lub pełnomocnictw, listy podmiotów należących do tej samej grupy kapitałowej lub nie wyraził zgody na poprawienie omyłki, co powodowało brak możliwości wybrania oferty złożonej przez wykonawcę jako najkorzystniejszej.

5. Zamawiający zatrzymuje wadium wraz z odsetkami, jeżeli Wykonawca, którego oferta została wybrana:
1) odmówił podpisania umowy w sprawie zamówienia publicznego na warunkach określonych w ofercie;
2) nie wniósł wymaganego zabezpieczenia należytego wykonania umowy;
3) zawarcie umowy w sprawie zamówienia stało się niemożliwe z przyczyn leżących po stronie Wykonawcy.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Rozdział XIII
Zabezpieczenie należytego wykonania umowy

1. Zabezpieczenie należytego wykonania umowy
   Przed podpisaniem umowy Oferent dostarczy Zamawiającemu zabezpieczenie należytego wykonania umowy w wysokości 5 % ceny całkowitej podanej w ofercie w jednej z poniżej wymienionych form:
   - pieniądzu – przelewem na rachunek Bank PKO BP SA na rachunek numer 30 1020 1026 0000 1402 0262 4336
   - gwarancjach bankowych,
   - gwarancjach ubezpieczeniowych,
2. Zamawiający zwróci 100 % zabezpieczenia na pisemny wniosek Wykonawcy w terminie 30 dni od dnia wykonania umowy i uznania przez Zamawiającego za należycie wykonane, potwierdzone protokołem odbioru.

Rozdział XIV
Informacje dotyczące miejsca, terminu składania, otwarcia Ofert oraz związania Ofertą

1. Termin składania Ofert upływa **07.08.2026 roku o godzinie 10:^{45}**
2. Oferty należy złożyć w siedzibie Przedsiębiorstwa Wodociągów i Kanalizacji Sp. z o.o. w Wołominie ul. Graniczna 1 w sekretariacie.
3. Oferty złożone po terminie zwraca się bez otwierania po upływie terminu wyznaczonego do składania Ofert.
4. Termin związania Ofertą wynosi 60 dni.
5. Bieg terminu rozpoczyna się wraz z upływem terminu składania Ofert.
6. Otwarcie Ofert jest jawne i nastąpi dnia **07.08.2026 roku o godzinie 11^{00}** w siedzibie Zamawiającego przy ul. Granicznej 1 w Wołominie.
7. Wszyscy zainteresowani mogą być obecni przy otwieraniu Ofert. W przypadku nieobecności Wykonawcy przy otwieraniu Ofert, Zamawiający prześle Wykonawcy informację z otwarcia Ofert na jego pisemny wniosek.
8. Podczas otwarcia zostaną ogłoszone:
   a. skład komisji przetargowej,
   b. kwota jaką Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia,
   c. nazwy i adresy Oferentów,
   d. ceny ofert.
9. Oferty zostaną sprawdzone czy zostały sporządzone zgodnie ze specyfikacją warunków zamówienia.
10. Zamawiający przyzna zamówienie Oferentowi, którego oferta spełnia wymagania określone w specyfikacji warunków zamówienia oraz została uznana za najkorzystniejszą.
11. W toku oceniania ofert zamawiający może zażądać od Oferentów udzielenia wyjaśnień dokumentów potwierdzających spełnienie warunków. Dokumenty mają być składane z datą nie późniejszą niż data składania wyjaśnień, a wyjaśnienia z datą na dzień składania wyjaśnień.
12. Zamawiający poprawia w ofercie:
    a. oczywiste omyłki pisarskie,
    b. oczywiste omyłki rachunkowe z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
    c. inne omyłki polegające na niezgodności oferty ze specyfikacją warunków zamówienia, niepowodujące istotnych zmian w treści oferty – niezwłocznie zawiadamiając o tym wykonawcę, którego oferta została poprawiona.

4

13. Zamawiający poprawiając omyłki rachunkowe zgodnie z założeniem niniejszego rozdziału uwzględnia konsekwencje rachunkowe dokonanych poprawek.
14. Zamawiający unieważnia postępowanie o udzielenie zamówienia, jeżeli:
    a. nie złożono żadnej oferty niepodlegającej odrzuceniu;
    b. cena najkorzystniejszej oferty przewyższa kwotę, którą Zamawiający zamierza przeznaczyć na sfinalizowanie zamówienia, chyba, że Zamawiający może zwiększyć tę kwotę do ceny najkorzystniejszej oferty;
    c. w przypadkach, kiedy zostały złożone oferty dodatkowe o takiej samej cenie;
    d. wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonanie zamówienia nie leży w interesie Zamawiającego, czego nie można było wcześniej przewidzieć;
    e. postępowanie obarczone jest niemożliwą do usunięcia wadą uniemożliwiającą zawarcie ważnej umowy w sprawie zamówienia.
15. Zamawiający może unieważnić postępowanie bez podania przyczyny zgodnie z art.70^1 §3 K.c.
16. O unieważnieniu postępowania zawiadamia się niezwłocznie wszystkich Oferentów.
17. W przypadku wykluczenia Oferenta lub odrzucenia oferty, zamawiający zawiadamia niezwłocznie Oferenta, którego ofertę odrzucił, podając uzasadnienie faktyczne i prawne wykonanej czynności.

Rozdział XV
Umowa

1. Zamawiający wezwie Oferenta w terminie 5 dni kalendarzowych od daty rozstrzygnięcia postępowania do podpisania Umowy.
2. Wybrany Oferent ma obowiązek skontaktować się w terminie do 3 dni roboczych od momentu powiadomienia go o wybraniu oferty.
3. Osoby reprezentujące Wykonawcę przy podpisywaniu umowy powinny posiadać ze sobą dokumenty potwierdzające ich umocowanie do podpisania umowy, o ile umocowanie to nie będzie wynikać z dokumentów załączonych do oferty.
4. Wzór umowy. Projekt umowy stanowi dodatek nr 5 do SWZ. W projekcie umowy zostanie wyznaczona wysokość kar umownych z tytułu niewykonania lub nienależytego wykonania umowy.

Rozdział XVI
Odwołania

1. Pouczenie o środkach odwoławczych przysługujących Wykonawcy w toku postępowania o udzielenie zamówienia.
2. Oferentom, których interes prawny doznał uszczerbku w wyniku naruszenia przez Zamawiającego zasad określonych w SWZ, przysługuje odwołanie skierowane do Zamawiającego.
3. Odwołanie należy wnieść nie później niż w ciągu 4 dni kalendarzowych od ogłoszenia wyniku postępowania.
4. Zamawiający rozpatrzy odwołanie w ciągu 4 dni kalendarzowych od złożenia i udzieli odpowiedzi na piśmie.

Dodatki do SWZ:

1) Dodatek nr 1 do SWZ – Opis przedmiotu zamówienia
2) Dodatek nr 2 do SWZ – Wzór formularza oferty
3) Dodatek nr 3 do SWZ – Oświadczenie o zapoznaniu się z SWZ
4) Dodatek nr 4 do SWZ – Oświadczenie o braku podstaw do wykluczenia
5) Dodatek nr 5 do SWZ – Wzór umowy
6) Dodatek nr 6 do SWZ – Upoważnienie do podpisania oferty
7) Dodatek nr 7 do SWZ – Lista podmiotów – Grupa kapitałowa
8) Dodatek nr 8 do SWZ – Klauzula Informacyjna
9) Dodatek nr 9 do SWZ – Oświadczenie art. 7 ust.1 Ustawy z dnia 13 kwietnia 2022 r.

Sporządziła: Urszula Papiór
Dział Inwestycji i Zamówień

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Dodatek nr 1 do SWZ
Opis przedmiotu zamówienia

OPIS PRZEDMIOTU ZAMÓWIENIA

Opracowanie dokumentacji i wykonanie audytów:
1: Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Przedmiotem usługi jest opracowanie oraz wsparcie we wdrożeniu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) u Zamawiającego. Usługa ma charakter jednorazowy i kończy się przekazaniem odebraniem gotowej dokumentacji wraz ze wsparciem eksperckim w toku procesu wdrożeniowego.

Wykonawca opracowuje dokumentację SZBI obejmującą politykę bezpieczeństwa informacji oraz kluczowe polityki tematyczne dostosowane do specyfiki operatora wodociągowego — w szczególności dotyczące kontroli dostępu do systemów IT i OT, zarządzania incydentami bezpieczeństwa (w tym incydentami zgłaszanymi do właściwego CSIRT zgodnie z uoKSC), bezpieczeństwa pracy zdalnej i urządzeń mobilnych, zarządzania kopiami zapasowymi oraz bezpieczeństwa relacji z dostawcami i wykonawcami zewnętrznymi. Liczba i szczegółowość opracowywanych dokumentów powinna wynika z analizy organizacji i powinna zostać uzgodniona z Zamawiającym przed przystąpieniem do właściwych prac. Wykonawca opracowuje dokumentację SZBI skoncentrowaną na kluczowych, praktycznych elementach możliwych do wdrożenia i utrzymania przez Zamawiającego. Zakres dokumentacji jest ograniczony do uzgodnionych obszarów i może nie obejmować wszystkich zabezpieczeń z Załącznika A normy ISO/IEC 27001 ma jednak pokrywać wymagania UoKSC.

W ramach usługi Wykonawca przeprowadzi wspólnie, w formie warsztatowej, z Zamawiającym wstępne szacowanie ryzyka obejmujące inwentaryzację kluczowych aktywów informacyjnych i systemów teleinformatycznych, identyfikację głównych zagrożeń istotnych dla operatora wodociągowego (w tym zagrożeń dla ciągłości dostaw wody i integralności systemów sterowania) oraz opracowanie uproszczonego Planu Postępowania z Ryzykiem wskazującego priorytety działań. Szacowanie ryzyka jest realizowane w ujęciu uproszczonym, ukierunkowanym na identyfikację kluczowych aktywów, zagrożeń i priorytetów postępowania z ryzykiem, z uwzględnieniem skali oraz kontekstu Zamawiającego. Metodyka pracy jest dostosowana do potrzeb projektu i może nie obejmować wszystkich elementów podejścia zgodnego z ISO/IEC 27005.W trakcie wdrożenia Wykonawca zapewnia wsparcie merytoryczne. Wsparcie obejmuje konsultacje dotyczące stosowania opracowanej dokumentacji oraz pomoc w przygotowaniu personelu do jej użytkowania.

Integralnym elementem usługi jest przeszkolenie kluczowego personelu Zamawiającego obejmujące omówienie struktury systemu zarządzania, sposobu stosowania kluczowych polityk i procedur oraz podstaw prowadzenia przeglądu dokumentacji. Szkolenie ma na celu wyposażenie wyznaczonych pracowników w wiedzę niezbędną do samodzielnego posługiwania się przekazaną dokumentacją.

Dokumentacja SZBI jest opracowywana z uwzględnieniem wymagań ustawy o krajowym systemie cyberbezpieczeństwa, Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych

Ram Interoperacyjności oraz normy PN-EN ISO/IEC 27001:2023 jako punktu odniesienia dla dobrych praktyk w zakresie zarządzania bezpieczeństwem informacji.

Zamawiający oczekuje, że rezultatem usługi będzie przekazanie dokumentacji SZBI dostosowanej do skali i specyfiki Zamawiającego, wraz z rekomendacjami dotyczącymi dalszego podnoszenia poziomu bezpieczeństwa.

2: Opracowanie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP) dla STI

Przedmiotem usługi jest pomoc w opracowaniu oraz wsparcie we wdrożeniu Planów Ciągłości Działania (BCP) i Planów Odtwarzania po Awarii (DRP) dla systemów teleinformatycznych (STI) Zamawiającego. Plany będą stanowić dokumenty operacyjne określające konkretne działania, sekwencje kroków, role personelu i zasoby niezbędne do utrzymania lub przywrócenia sprawności krytycznych systemów IT w przypadku awarii lub zakłócenia. Usługa jest realizowana jako projekt o zdefiniowanym zakresie i terminie zakończenia.

Etap wstępny będzie obejmował identyfikację systemów teleinformatycznych kluczowych dla utrzymania ciągłości usługi wodociągowej, przegląd istniejących rozwiązań w zakresie kopii zapasowych i redundancji IT oraz rozpoznanie kluczowych zależności między systemami IT a procesami operacyjnymi Zamawiającego. Na tej podstawie Wykonawca wspólnie z Zamawiającym wybierze dwa kluczowe, reprezentatywne systemy (przypadki wzorcowe), dla których zostaną opracowane przykładowe plany BCP i DRP oraz ujednolicone procedury towarzyszące, co definiuje zamknięty zakres usługi.

Kluczowym elementem usługi jest przeprowadzenie warsztatowej analizy wpływu na działalność (BIA) wspólnie z wyznaczonymi przedstawicielami Zamawiającego. Warsztaty służą wyznaczeniu dla dwóch wybranych systemów (przypadków wzorcowych): orientacyjnego Docelowego Czasu Odtworzenia (RTO), orientacyjnego Docelowego Punktu Odtworzenia (RPO) oraz priorytetu odtwarzania. Wyniki BIA będą dokumentowane i będą stanowiły bezpośrednią podstawę projektowania treści planów. Jeżeli w toku warsztatów nie będzie możliwe uzyskanie danych niezbędnych dla konkretnego systemu, Wykonawca odnotuje przyjęte założenia zastępcze i uzgodni z Zamawiającym sposób postępowania — np. zawężenie zakresu planu lub opisanie ograniczeń przyjętych przy jego opracowaniu.

Na podstawie wyników analizy BIA Wykonawca wspólnie z Zamawiającym opracowuje dla dwóch wybranych systemów (w ujęciu wzorcowym) Plan Ciągłości Działania (BCP) określający procedury postępowania w trakcie trwania zakłócenia — w tym tryb pracy awaryjnej, zastępcze sposoby realizacji funkcji systemu oraz zasady komunikacji wewnętrznej i eskalacji — oraz Plan Odtwarzania po Awarii (DRP) określający krok po kroku procedury technicznego przywrócenia sprawności systemu po zakończeniu zakłócenia, wymagane zasoby i narzędzia, role techniczne personelu oraz kryteria zakończenia procesu odtwarzania. Uzupełnieniem planów są ujednolicone procedury zarządzania kopiami zapasowymi, zapewniające spójność z parametrami RPO przyjętymi w analizie BIA.

W toku wdrożenia Wykonawca przeprowadzi szkolenie dla wyznaczonego przez Zamawiającego personelu, obejmujące omówienie struktury i logiki opracowanych planów, sposobu ich stosowania w praktyce oraz zasad ich aktualizacji. Ponadto Wykonawca wspólnie z Zamawiającym przeprowadza jedno ćwiczenie stołowe (table-top) dla jednego z opracowanych planów, demonstrując praktycznie przebieg testu i sposób dokumentowania jego wyników. Ćwiczenie to ma charakter instruktażowy i stanowi wzorzec dla samodzielnego przeprowadzania kolejnych testów

przez Zamawiającego. Regularne testy pozostałych planów będą realizowane przez Zamawiającego we własnym zakresie po zakończeniu usługi.

Plany są opracowywane z uwzględnieniem wymagań ustawy o krajowym systemie cyberbezpieczeństwa, Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności oraz normy PN-EN ISO 22301 jako punktu odniesienia dla dobrych praktyk w zakresie planowania ciągłości działania.

Rezultatem usługi jest przekazanie Zamawiającemu zamkniętego zestawu planów BCP i DRP dla uzgodnionych systemów STI, gotowych do bezpośredniego stosowania przez personel Zamawiającego, wraz z rekomendacjami dotyczącymi dalszego utrzymania i rozwijania dokumentacji.

3: Audyt KRI, Audyt SZBI, Audyt ciągłości działania

3.1: Audyt KRI

Realizacja audytu bezpieczeństwa informacji będzie prowadzona jako audyt zgodności systemów organizacyjnych oraz technicznych z obowiązującymi wymaganiami Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej.

Audyt zostanie przeprowadzony w oparciu o metodykę audytową określoną w normie PN-EN ISO 19011:2018, stanowiącej międzynarodowy standard w zakresie planowania, realizacji, dokumentowania oraz raportowania audytów systemów zarządzania. W toku realizacji czynności audytowych zastosowane zostaną zasady niezależności, bezstronności, podejścia opartego na dowodach oraz podejścia systemowego, umożliwiające kompleksową ocenę dojrzałości organizacyjnej oraz skuteczności wdrożonych mechanizmów bezpieczeństwa informacji.

Jednocześnie zakres merytoryczny audytu zostanie ukształtowany w oparciu o wybrane wymagania i dobre praktyki wynikające z normy PN-EN ISO/IEC 27001:2023, w szczególności w obszarach zarządzania ryzykiem bezpieczeństwa informacji, organizacyjnych i technicznych środków ochrony informacji, zarządzania dostępem do zasobów teleinformatycznych, monitorowania zdarzeń bezpieczeństwa, realizacji kopii zapasowych oraz zapewnienia ciągłości działania systemów informatycznych. Norma ISO/IEC 27001 będzie stanowiła referencyjny punkt odniesienia dla oceny adekwatności i proporcjonalności stosowanych zabezpieczeń w relacji do zidentyfikowanych zagrożeń i poziomu ryzyka.

Audyt zostanie zrealizowany w formie audytu na miejscu (on-site) w siedzibie Zamawiającego. Zakres prac obejmować będzie przeprowadzenie szczegółowej analizy dokumentacji systemowej i proceduralnej, w tym polityk bezpieczeństwa informacji, procedur zarządzania incydentami, analiz ryzyka, rejestrów uprawnień, ewidencji aktywów oraz dokumentacji technicznej środowiska teleinformatycznego. Uzupełnieniem analizy dokumentacyjnej będą wywiady audytowe z odpowiednimi osobami, a także wyrywkowa weryfikacja wybranych elementów infrastruktury i stanowisk pracy pod kątem zgodności z przyjętymi regulacjami oraz dobrymi praktykami bezpieczeństwa IT.

Przeprowadzone czynności audytowe umożliwią dokonanie kompleksowej oceny stopnia spełnienia minimalnych wymagań wynikających z Krajowych Ram Interoperacyjności.

Efektem audytu będzie sporządzenie raportu końcowego zawierającego syntetyczną ocenę poziomu zgodności, identyfikację stwierdzonych niezgodności, luk i obszarów podwyższonego ryzyka, a także zestaw rekomendacji ukierunkowanych na podniesienie poziomu bezpieczeństwa informacji oraz zapewnienie pełnej zgodności regulacyjnej. Raport stanowić będzie formalny dokument potwierdzający realizację obowiązków audytowych wynikających z przepisów prawa oraz podstawę do planowania dalszych działań organizacyjnych i technicznych w obszarze cyberbezpieczeństwa.

Audyt zostanie przeprowadzony przez zespół audytorów posiadających kwalifikacje i doświadczenie w zakresie audytów bezpieczeństwa informacji, stosowania metodyki ISO 19011 oraz wdrażania i oceny systemów zarządzania bezpieczeństwem informacji zgodnych z normą ISO/IEC 27001, co zapewni wysoką jakość merytoryczną oraz wiarygodność uzyskanych wyników.

3.2: Audyt SZBI wg ISO27001

Realizacja audytu bezpieczeństwa informacji będzie prowadzona jako audyt zgodności systemów organizacyjnych oraz technicznych z obowiązującymi wymaganiami Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej.

Audyt zostanie przeprowadzony w oparciu o metodykę audytową określoną w normie PN-EN ISO 19011:2018, stanowiącej międzynarodowy standard w zakresie planowania, realizacji, dokumentowania oraz raportowania audytów systemów zarządzania. W toku realizacji czynności audytowych zastosowane zostaną zasady niezależności, bezstronności, podejścia opartego na dowodach oraz podejścia systemowego, umożliwiające kompleksową ocenę dojrzałości organizacyjnej oraz skuteczności wdrożonych mechanizmów bezpieczeństwa informacji.

Jednocześnie zakres merytoryczny audytu zostanie ukształtowany w oparciu o wybrane wymagania i dobre praktyki wynikające z normy PN-EN ISO/IEC 27001:2023, w szczególności w obszarach zarządzania ryzykiem bezpieczeństwa informacji, organizacyjnych i technicznych środków ochrony informacji, zarządzania dostępem do zasobów teleinformatycznych, monitorowania zdarzeń bezpieczeństwa, realizacji kopii zapasowych oraz zapewnienia ciągłości działania systemów informatycznych.

Norma ISO/IEC 27001 będzie stanowiła referencyjny punkt odniesienia dla oceny adekwatności i proporcjonalności stosowanych zabezpieczeń w relacji do zidentyfikowanych zagrożeń i poziomu ryzyka.

Audyt zostanie zrealizowany w formie audytu na miejscu (on-site) w siedzibie Zamawiającego. Zakres prac obejmować będzie przeprowadzenie szczegółowej analizy dokumentacji systemowej i proceduralnej, w tym polityk bezpieczeństwa informacji, procedur zarządzania incydentami, analiz ryzyka, rejestrów uprawnień, ewidencji aktywów oraz dokumentacji technicznej środowiska teleinformatycznego. Uzupełnieniem analizy dokumentacyjnej będą wywiady audytowe z odpowiednimi osobami, a także wyrywkowa weryfikacja wybranych elementów infrastruktury i stanowisk pracy pod kątem zgodności z przyjętymi regulacjami oraz dobrymi praktykami bezpieczeństwa IT.

Przeprowadzone czynności audytowe umożliwią dokonanie kompleksowej oceny stopnia spełnienia minimalnych wymagań wynikających z Krajowych Ram Interoperacyjności.

Efektem audytu będzie sporządzenie raportu końcowego zawierającego syntetyczną ocenę poziomu zgodności, identyfikację stwierdzonych niezgodności, luk i obszarów podwyższonego ryzyka, a także

4

zestaw rekomendacji ukierunkowanych na podniesienie poziomu bezpieczeństwa informacji oraz zapewnienie pełnej zgodności regulacyjnej. Raport stanowić będzie formalny dokument potwierdzający realizację obowiązków audytowych wynikających z przepisów prawa oraz podstawę do planowania dalszych działań organizacyjnych i technicznych w obszarze cyberbezpieczeństwa.

Audyt zostanie przeprowadzony przez zespół audytorów posiadających kwalifikacje i doświadczenie w zakresie audytów bezpieczeństwa informacji, stosowania metodyki ISO 19011 oraz wdrażania i oceny systemów zarządzania bezpieczeństwem informacji zgodnych z normą ISO/IEC 27001, co zapewni wysoką jakość merytoryczną oraz wiarygodność uzyskanych wyników.

3.3: Audyt SZCD STI wg ISO 22301

Przegląd Systemu Zarządzania Ciągłością Działania (SZCD) dla Systemów Teleinformatycznych i Infrastruktury (STI) zgodnie z ISO 22301:2019

Przedmiotem zamówienia jest wykonanie przeglądu Systemu Zarządzania Ciągłością Działania (SZCD) wdrożonego w organizacji Zamawiającego, w zakresie systemów teleinformatycznych (IT), systemów technologicznych (OT/SCADA) oraz usług świadczonych z wykorzystaniem infrastruktury teleinformatycznej (STI), pod kątem zgodności z wymaganiami normy ISO 22301:2019. Przegląd nie stanowi audytu certyfikacyjnego, audytu technicznego, oceny bezpieczeństwa systemów IT i OT.

Celem realizacji zamówienia jest:

1. Ocena zgodności SZCD z wymaganiami normy ISO 22301:2019;
2. Weryfikacja skuteczności przyjętych rozwiązań organizacyjnych, technicznych i proceduralnych;
3. Identyfikacja luk i obszarów wymagających doskonalenia;
4. Przygotowanie rekomendacji działań usprawniających.

Zamawiający wymaga, by ocena zgodności objęła wszystkie obszary normy ISO 22301:2019 (rozdziały 4–10). Zamawiający wymaga, by w ramach prac Wykonawca dokonał przeglądu dokumentacji obejmującej kontekst organizacji (w tym przynajmniej: zakres funkcjonowania SZCD, kontekst wewnętrzny i zewnętrzny, identyfikacja stron zainteresowanych, wymagania prawne i regulacyjne, zgodność zakresu SZCD z działalnością przedsiębiorstwa) oraz dokumentacji SZCD udostępnionej przez Zamawiającego.

Przegląd dokumentacji SZCD obejmie w szczególności: Politykę Ciągłości Działania, cele SZCD oraz przypisanie ról, odpowiedzialności i uprawnień; zakres systemu; analizę wpływu na działalność (BIA) wraz z parametrami czasowymi (MTPD, RTO); ocenę ryzyka zakłóceń działań krytycznych, a także ryzyka i szanse odnoszące się do samego systemu zarządzania; przyjęte strategie i rozwiązania ciągłości działania wraz z wymaganiami dotyczącymi zasobów oraz parametrami RTO, RPO i MBCO; plany ciągłości działania (BCP) i plany odtworzeniowe IT (DRP); strukturę reagowania oraz procedury ostrzegania i komunikacji w sytuacji zakłócenia; procedury testowania i ćwiczeń; procedury przeglądów i doskonalenia. Przeglądowi podlegają również zapisy potwierdzające funkcjonowanie systemu, w tym dowody kompetencji i świadomości personelu, wskaźniki i wyniki monitorowania skuteczności SZCD, zapisy z audytów wewnętrznych i przeglądów zarządzania oraz rejestr niezgodności i działań korygujących. Zamawiający udostępni także rejestry usług krytycznych, zasobów ryzyk oraz dokumentację dotyczącą dostawców usług krytycznych).

Wykonawca wykona także przegląd infrastruktury IT i OT, w tym: zakresie niezbędnym do potwierdzenia spełnienia wymagań ISO 22301, rozumianym jako przegląd istnienia i skuteczności mechanizmów istotnych dla ciągłości działania.

Przegląd obejmie:

1. obszar IT: serwery, macierze dyskowe, systemy kopii zapasowych, środowiska wirtualne, sieć LAN/WAN, systemy bezpieczeństwa, Active Directory, usługi chmurowe, system ERP, system bilingowy, GIS.
2. obszar OT: systemy SCADA; sterowniki PLC; systemy telemetryczne; systemy monitoringu sieci; systemy sterowania pompowniami; systemy sterowania stacjami uzdatniania; systemy sterowania oczyszczalniami.

W czasie realizacji przeglądu Wykonawca dokona analizę dokumentacji Zamawiającego, przeprowadzi wywiady z przedstawicielami Zamawiającego; zweryfikuje konfiguracje wybranych systemów (w zakresie niezbędnym dla potwierdzenia spełnienia wymagań ISO 22301), zbierze dowody na funkcjonowanie SZCD, przeprowadzi analizę wyników ćwiczeń i testów. Przegląd odbędzie się on-site, wraz z wizją lokalną w wybranych obiektach Zamawiającego.

Po zakończonym przeglądzie, Wykonawca dostarczy raport, zawierający ocenę zgodności z ISO 22301, wykaz niezgodności, obserwacji oraz ryzyk, a także rekomendacje działań doskonalących.

Wykonawca wskaże dla każdej zidentyfikowanej niezgodności opis, poziom ryzyka, rekomendowane działania oraz priorytet realizacji.

Zamawiający wymaga, by raport został zaprezentowany na spotkaniu zamykającym z kierownictwem Zamawiającego.

Osoby skierowane do realizacji zamówienia powinny posiadać doświadczenie w:

1. audytowaniu lub wdrażaniu systemów zgodnych z ISO 22301;
2. ocenie środowisk IT oraz OT/SCADA;
3. prowadzeniu audytów systemów zarządzania.

4: Testy bezpieczeństwa

4.1: Testy bezpieczeństwa infrastruktury sieciowej IT/OT/ICS/IIoT

Wykonawca zobowiązany jest do przeprowadzenia testu penetracyjnego infrastruktury Zamawiającego w metodyce gray-box, w taki sposób, aby poprzez próbę przełamania zabezpieczeń umożliwić identyfikację ryzyk oraz potencjalnych konsekwencji ewentualnego włamania. Test penetracyjny musi być wykonywany zarówno manualnie, jak i automatycznie, z wykorzystaniem specjalistycznych narzędzi oraz własnych skryptów przygotowanych na podstawie wiedzy i doświadczeń Wykonawcy. Testy muszą zostać przeprowadzone w oparciu o metodologię OSSTMM (Open Source Security Testing Methodology Manual) lub równoważną, przy zapewnieniu co najmniej równoważnego zakresu i poziomu szczegółowości.

Metoda równoważna musi zapewniać co najmniej ten sam poziom jakości, pokrycia i rygoru testów. Dotyczy to poniższych kluczowych kryteriów:

1) metodyka działania powinna jasno definiować:

a) etapy testów (planowanie, rekonesans, testy właściwe, raportowanie),

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

b) podejście do identyfikacji podatności,
c) sposób weryfikacji i potwierdzania wyników (brak „false positives").

2) poziom szczegółowości:

a) testy nie mogą być powierzchowne (np. tylko skan automatyczny),
b) wymagane są techniki manualne i analiza ekspercka,
c) opis podatności musi zawierać dowody, wpływ i rekomendacje.

3) powtarzalność i mierzalność:

a) metodologia powinna umożliwiać odtworzenie testów,
b) metodologia powinna zawierać sposób oceny ryzyka lub klasyfikacji podatności.

Wykonawca zobowiązany jest do realizacji testów penetracyjnych infrastruktury w co najmniej dwóch fazach: zewnętrznej i wewnętrznej. Wewnętrzna ocena bezpieczeństwa infrastruktury powinna umożliwiać identyfikację wewnętrznych ryzyk występujących w organizacji. Testy wewnętrzne mogą być realizowane zdalnie.

Test penetracyjny infrastruktury musi umożliwić identyfikację istniejących podatności oraz dostarczyć praktyczne dowody czy podatności te mogą zostać wykorzystane.

W ramach realizacji zamówienia Wykonawca zobowiązany jest do wykonania co najmniej następujących czynności:

1) Skanowanie sieci.
2) Weryfikacja domyślnych haseł w usługach umożliwiających logowanie.
3) Wykrycie możliwości przechwycenia haseł w sieci oraz weryfikacja pod kątem możliwości złamania haseł.
4) Testowanie bezpieczeństwa urządzeń drukujących.
5) Testowanie konfiguracji protokołów Secure Socket Layer (SSL) / Transport Layer Security (TLS). Sprawdzenie czy konfiguracja serwera nie zezwala na wykorzystanie starszych wersji protokołów TLS lub SSL oraz zweryfikowanie, czy nie jest możliwe korzystanie ze słabych algorytmów szyfrowania, które potencjalnie można rozszyfrować.
6) Testowanie usług sieciowych (w szczególności FTP, SSH, Telnet, SMTP, POP3, SMB itp.).
7) Przeprowadzenie działań typu spoofing (ataku polegającego na fałszowaniu lub modyfikowaniu danych w celu przejęcia tożsamości lub podszywania się pod inną osobę, system lub urządzenie w celu oszustwa lub uzyskania nieautoryzowanego dostępu).
8) Weryfikacja możliwości uzyskania dostępu do współdzielonych zasobów.
9) Testowanie bezpieczeństwa sieci bezprzewodowych (WiFi) jeżeli występuje w lokalizacji.
10) Testowanie bezpieczeństwa baz danych w zakresie brute force i podatności
11) Identyfikacja podatności w usługach sieciowych i aplikacjach docelowych.
12) Wykorzystanie zidentyfikowanych podatności przy użyciu odpowiednich narzędzi, skryptów i metod, w zakresie uzgodnionym z Zamawiającym.

4.2: Testy bezpieczeństwa serwisów internetowych IT/OT/ICS

Testy bezpieczeństwa zostaną przeprowadzone w metodyce gray-box, tj. z ograniczoną wiedzą o systemie.

Test będzie realizowany zgodnie z uznanymi standardami branżowymi w zakresie testów bezpieczeństwa aplikacji i serwisów webowych, w szczególności:

1) OWASP Top 10,
2) OWASP Web Security Testing Guide

lub standardami równoważnymi obejmującymi wskazane kategorie podatności.

W ramach testów Wykonawca dokona weryfikacji podatności w szczególności w zakresie:

1) Injection – podatności związanych z wstrzyknięciami (np. SQL Injection, Command Injection),
2) Broken Authentication and Session Management – słabości mechanizmów uwierzytelniania oraz zarządzania sesją,
3) Cross-Site Scripting (XSS) – podatności na ataki typu XSS,
4) Insecure Direct Object References – nieautoryzowanego dostępu do zasobów poprzez manipulację identyfikatorami obiektów,
5) Security Misconfiguration – błędów konfiguracji bezpieczeństwa,
6) Sensitive Data Exposure – niewłaściwej ochrony danych wrażliwych,
7) Missing Function Level Access Control – błędów w kontroli dostępu do funkcji systemu,
8) Cross-Site Request Forgery (CSRF) – podatności na ataki CSRF,
9) Using Components with Known Vulnerabilities – wykorzystania komponentów zawierających znane podatności,
10) Unvalidated Redirects and Forwards – nieprawidłowej walidacji przekierowań.

Testy będą prowadzone z wykorzystaniem metod manualnych oraz narzędzi wspomagających, przy czym zautomatyzowane skanery podatności nie będą stanowiły jedynej metody badawczej.

1. Zasady bezpieczeństwa prowadzenia testów

Testy nie obejmują:

1) testów destrukcyjnych,
2) testów typu Denial of Service (DoS),
3) wprowadzania zmian konfiguracyjnych w środowisku Zamawiającego.

W przypadku wykrycia podatności o krytycznym poziomie ryzyka, Wykonawca zobowiązany jest do:

1) niezwłocznego poinformowania Zamawiającego,
2) udokumentowania podatności w sposób umożliwiający jej weryfikację,
3) czasowego wstrzymania dalszych testów bezpieczeństwa w zakresie mogącym wpływać na stabilność systemu.

Kontynuacja audytu nastąpi po podjęciu decyzji przez Zamawiającego dotyczącej dalszego sposobu prowadzenia testów.

2. Wyniki testów – raporty

Po zakończeniu testów Wykonawca przygotuje raporty z audytu bezpieczeństwa zawierający co najmniej:

1) opis metodyki przeprowadzonych testów,
2) wykaz zidentyfikowanych podatności,
3) klasyfikację podatności według poziomu ryzyka (np. CVSS Common Vulnerability Scoring System lub równoważnego standardu),
4) opis scenariusza wykorzystania podatności (proof-of-concept),
5) ocenę wpływu podatności na bezpieczeństwo systemu,
6) rekomendacje działań naprawczych.

Raporty zostaną przekazane w formie elektronicznej. Po przekazaniu raportów Wykonawca zobowiązuje się do nieprzechowywania danych po zakończeniu zamówienia.

Wymagania dla Wykonawcy:

1. Certyfikacja instytucjonalna Wykonawcy

Wykonawca musi posiadać aktualne certyfikaty potwierdzające, że jego własna organizacja funkcjonuje zgodnie z następującymi standardami zarządzania: normą ISO 9001, normą ISO/IEC 27001 oraz normą ISO 22301. Wymóg ten ma na celu zapewnienie, że podmiot odpowiedzialny za wdrażanie systemów zarządzania u Zamawiającego sam stosuje te standardy we własnej działalności. Każdy z wymaganych certyfikatów musi być wydany przez jednostkę certyfikującą akredytowaną przez Polskie Centrum Akredytacji (PCA) lub przez jednostkę akredytowaną przez organizację będącą sygnatariuszem porozumienia EA MLA (European Cooperation for Accreditation — Multilateral Agreement) lub IAF MLA (International Accreditation Forum — Multilateral Agreement). Zamawiający dopuszcza certyfikaty równoważne wystawione przez jednostki spełniające powyższe kryterium akredytacji — ciężar wykazania równoważności spoczywa na Wykonawcy.

Na potwierdzenie spełniania tego warunku udziału w postępowaniu, Zamawiający przed wyborem najkorzystniejszej oferty wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie kopii wszystkich trzech certyfikatów wraz z zakresem certyfikacji i datą ważności

W przypadku certyfikatów równoważnych Wykonawca składa na wezwanie ponadto dokument potwierdzający akredytację jednostki certyfikującej oraz pisemne uzasadnienie równoważności. Jeżeli wykonawca nie złoży żądanych certyfikatów lub dokumentów potwierdzających ich równoważność, są one niekompletne lub zawierają błędy, Zamawiający wezwie wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w wyznaczonym terminie.

2. Warunki udziału w postępowaniu – Zdolność techniczna lub zawodowa

1. Zamawiający uzna warunek zdolności technicznej lub zawodowej za spełniony, jeżeli Wykonawca wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert wykonał należycie:
   a) w zakresie wdrożenia systemów (SZBI lub BCP/DRP): co najmniej 2 (dwie) usługi, z których każda polegała na opracowaniu dokumentacji i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) lub opracowaniu planów ciągłości działania (BCP/DRP), o wartości nie mniejszej niż 40 000,00 zł brutto każda;
   b) w zakresie audytu: co najmniej 2 (dwie) usługi, z których każda polegała na przeprowadzeniu audytu bezpieczeństwa informacji lub audytu SZBI, o wartości nie mniejszej niż 20 000,00 zł brutto każda;
   c) w zakresie testów bezpieczeństwa: co najmniej 2 (dwie) usługi, z których każda obejmowała swoim zakresem przeprowadzenie testów penetracyjnych infrastruktury sieciowej oraz testów penetracyjnych aplikacji webowych, o wartości nie mniejszej niż 20 000,00 zł brutto każda.
2. Wykonawca musi dysponować na potrzeby realizacji zamówienia zespołem liczącym łącznie co najmniej 7 wykwalifikowanych osób, w skład którego wejdą specjaliści przypisani wyłącznie do jednej z trzech odrębnych grup funkcjonalnych:
   a) zespołu wdrożeniowego,
   b) zespołu audytowego,
   c) zespołu testów penetracyjnych.

3. Zamawiający bezwzględnie zakazuje łączenia ról i funkcji pomiędzy poszczególnymi grupami funkcjonalnymi. Oznacza to, że każda osoba skierowana do realizacji zamówienia może zostać przypisana tylko do jednego zespołu. W szczególności: specjalista realizujący testy penetracyjne nie może uczestniczyć w pracach wdrożeniowych ani audytowych, a członkowie zespołu wdrożeniowego nie mogą pełnić funkcji w zespole audytowym ani penetracyjnym. Minimalny skład osobowy musi składać się z 7 odrębnych osób fizycznych.
4. Zamawiający zastrzega obowiązek osobistego wykonania przez Wykonawcę kluczowych zadań polegających na pracach wdrożeniowych (tj. opracowanie i wdrożenie SZBI, BCP/DRP, SZCD) oraz przeprowadzeniu testów penetracyjnych infrastruktury i aplikacji. Tym samym Wykonawca może powierzyć podwykonawcom wyłącznie realizację zadań wchodzących w zakres audytów zewnętrznych (SZBI i SZCD).
5. Zamawiający wymaga zatrudnienia na podstawie stosunku pracy przez Wykonawcę osób wykonujących czynności w zakresie prac wdrożeniowych (opracowanie i wdrożenie SZBI, BCP/DRP, SZCD) oraz testów penetracyjnych infrastruktury i aplikacji.
6. Wymóg zatrudnienia na umowę o pracę, o którym mowa w ust. 4, nie dotyczy specjalistów realizujących audyty zewnętrzne. Ze względu na fakt, iż audytorzy mogą stanowić personel podwykonawcy, Zamawiający dopuszcza, aby osoby z zespołu audytowego realizowały swoje zadania na podstawie innych form współpracy (np. umów cywilnoprawnych, kontraktów B2B) zawartych z Wykonawcą lub podwykonawcą."
7. Zespół wdrożeniowy — SZBI, BCP/DRP, SZCD Zespół wdrożeniowy odpowiedzialny za opracowanie i wdrożenie dokumentacji SZBI, BCP/DRP oraz SZCD musi liczyć co najmniej 3 osoby zatrudnione przez Wykonawcę na podstawie umowy o pracę w rozumieniu ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy. Osoby z zespołu wdrożeniowego nie mogą uczestniczyć w realizacji prac zespołu audytowego ani zespołu testów penetracyjnych. Członkowie zespołu wdrożeniowego muszą łącznie posiadać następujące kwalifikacje (dopuszcza się łączenie poniższych wymogów przez te same osoby wewnątrz tego zespołu):
   a) Audytor Wiodący ds. Wdrożeń: posiada jednocześnie certyfikat Audytora Wiodącego ISO/IEC 27001 (Lead Auditor) lub równoważny, certyfikat Audytora Wiodącego ISO 22301 (Lead Auditor) lub równoważny oraz certyfikat CISA (Certified Information Systems Auditor) lub równoważny.
   b) Audytor Wspomagający ds. Wdrożeń: posiada co najmniej certyfikat Audytora ISO/IEC 27001 (Auditor) lub równoważny certyfikat Audytora Wiodącego ISO 22301 (Lead Auditor) lub równoważny
   c) Specjalista ds. infrastruktury i bezpieczeństwa OT/IT: posiada certyfikaty lub uprawnienia potwierdzające umiejętności w zakresie:
      i. umiejętności projektowania i wdrażania zabezpieczeń dla sieci przemysłowych (OT/ICS) (segmentacja sieci OT zgodnie z modelem Purdue, wykrywanie i profilowanie urządzeń przemysłowych, przeprowadzanie inspekcji protokołów przemysłowych (Modbus, DNP3, IEC 61850), wirtualne łatanie podatnych systemów bez przerywania ciągłości produkcji, kompetencje z zakresu centralnego monitorowania, korelacji zdarzeń bezpieczeństwa w środowiskach ICS/SCADA oraz oceny ryzyka OT
      ii. umiejętności konfiguracji i administracji firewallem nowej generacji (NGFW) – polityki bezpieczeństwa, filtrowanie ruchu, VPN (IPsec, SSL), IPS, uwierzytelnianie użytkowników i podstawowy monitoring.
      iii. znajomości sieci - potwierdzenie umiejętności w zakresie sieci komputerowych, konfiguracji i rozwiązywania problemów z urządzeniami sieciowymi (przełączniki,

routery), zrozumienie modeli OSI i TCP/IP, umiejętność wdrażania routingu (OSPF, EIGRP, statyczny), konfiguracji sieci VLAN i STP, zarządzania dostępem przez ACL oraz podstawowych usługach sieciowych (DHCP, DNS, NAT), podstawy bezpieczeństwa sieci, konfiguracji VPN, zarządzania pasmem oraz wprowadzenie do automatyzacji sieci i programowalności, kompetencje w obszarze administracji i konfiguracji infrastruktury sieciowej.

iv. uprawnień SEP E+D do 15 kV.

8. Zespół audytowy — audyty zewnętrzne SZBI, SZCD, KRI/uoKSC Zespół audytowy odpowiedzialny za przeprowadzenie audytów zewnętrznych musi liczyć co najmniej dwie osoby. Ze względu na niezależny charakter usług audytowych, Zamawiający nie wymaga zatrudnienia tych osób na podstawie umowy o pracę (dopuszczalne są formy współpracy na podstawie umów cywilnoprawnych, w tym z podwykonawcami). Osoby z zespołu audytowego nie mogą być tymi samymi osobami, które realizowały prace wdrożeniowe lub testy penetracyjne w ramach tego samego zamówienia.
   a) Pierwsza osoba (Audytor Wiodący ds. Audytów): musi posiadać jednocześnie certyfikat Audytora Wiodącego ISO/IEC 27001 (Lead Auditor) lub równoważny oraz certyfikat Audytora Wiodącego ISO 22301 (Lead Auditor) lub równoważny,
   b) Druga osoba (Audytor Wspomagający ds. Audytów): musi posiadać co najmniej certyfikat Audytora ISO/IEC 27001 (Auditor) lub równoważny.
9. Zespół testów penetracyjnych Zespół testów penetracyjnych musi liczyć co najmniej dwie osoby zatrudnione przez Wykonawcę na podstawie umowy o pracę w rozumieniu Kodeksu pracy. Osoby z zespołu testów penetracyjnych nie mogą uczestniczyć w realizacji prac zespołu wdrożeniowego ani zespołu audytowego w ramach tego samego zamówienia.
   a) Pierwsza osoba (Pentester Główny): musi posiadać jednocześnie certyfikat CEH (Certified Ethical Hacker) lub równoważny, certyfikat CISSP (Certified Information Systems Security Professional) lub równoważny oraz certyfikat eWPT (eLearnSecurity Web Application Penetration Tester) lub równoważny.
   b) Druga osoba (Pentester Wspomagający): musi posiadać co najmniej certyfikat CEH lub równoważny.

Termin realizacji: odbiór końcowy do 30 listopada 2026 roku

Wykonawca, w terminie 10 dni roboczych od dnia zawarcia umowy, przedłoży do zatwierdzenia Zamawiającemu harmonogram realizacji prac, obejmujący podział na etapy, terminy realizacji oraz planowane terminy odbiorów częściowych. Odbiory częściowe będą dokonywane po zakończeniu etapów wskazanych w zatwierdzonym harmonogramie. Na podstawie podpisanych protokołów odbioru częściowego Zamawiający dokona rozliczenia częściowego. Strony ustalają, że w ramach realizacji umowy dopuszcza się nie więcej niż dwa odbiory częściowe oraz odbiór końcowy.

Płatność:

W terminie 30 dni od daty otrzymania prawidłowo wystawionej faktury VAT.

Zamawiający dopuszcza płatność maksymalnie w trzech transzach:

1. Po odbiorze części I – Wykonanie testów bezpieczeństwa infrastruktury sieciowej IT/OT/ICS/IIoT i testów bezpieczeństwa serwisów internetowych IT/OT/ICS
2. Po odbiorze części II – Wykonanie Audytu KRI, Audytu SZBI, Audytu ciągłości działania

Cyberbezpieczne Wodociągi

Dodatek nr 2 do SWZ
Wzór formularza oferty

(pieczęć adresowa firmy oferenta)

OFERTA

Zamawiający:

Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o.
ul. Graniczna 1, 05-200 Wołomin
tel. (022) 776 21 21

Dane dotyczące oferenta:

Nazwa: .....

Siedziba: .....

Nr telefonu: .....

E- mail.....

Nr NIP.....

Nr REGON.....

Składamy niniejszą ofertę na ***„Opracowanie dokumentacji i wykonanie audytów – obszar organizacyjny w ramach projektu „Cyberbezpieczne Wodociągi" realizowanego przez Przedsiębiorstwo Wodociągów i Kanalizacji Sp.z o.o. w Wołominie, w ramach Inwestycji C3.1.1 „Cyberbezpieczeństwo – CyberPL" – Cyberbezpieczne Wodociągi, finansowanego z Krajowego Planu Odbudowy i Zwiększania Odporności"***

Całkowity koszt realizacji usługi wyniesie:

Wartość netto .....zł
(słownie: .....zł)
Wartość podatku VAT ..... zł
(słownie: .....zł)
Wartość brutto ..... zł
(słownie: .....zł)

W tym:

Lp.	Nazwa	wartość netto PLN	wartość VAT PLN	wartość brutto PLN
1	Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)			
2	Opracowanie planów ciągłości działania (BCP) i odtworzenia po awarii (DRP) dla STI			
3	Audyt zgodności KRI			

3. Po odbiorze końcowym - Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), Opracowanie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP) dla STI

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

4	Audyt SZBI			
5	Audyt ciągłości działania			
6	Testy bezpieczeństwa infrastruktury sieciowej IT/OT/ICS /IIoT			
7	Testy bezpieczeństwa serwisów internetowych IT/OT /ICS			
	Suma			

***Suma wartości z tabeli, musi być równa sumie wartości wpisaną w całkowity koszt realizacji usługi.**

Termin związania ofertą 60 dni. Bieg terminu rozpoczyna się wraz z upływem terminu składania ofert.

Oświadczamy, że:

1. *Zapoznaliśmy się ze specyfikacją warunków zamówienia i nie wnosimy do niej zastrzeżeń.*
2. *Akceptujemy wskazany w SWZ czas związania ofertą.*
3. *Zapoznaliśmy się z projektem umowy i nie wnosimy do niego żadnych uwag, w przypadku wyboru naszej oferty zobowiązujemy się do zawarcia umowy na wyżej wymienionych warunkach w miejscu i terminie wyznaczonym przez Zamawiającego*
4. *Zapoznaliśmy się z treścią Klauzuli informacyjnej dotyczącej przetwarzania danych osobowych i wyrażamy zgodę na ich przetwarzanie*
5. *Wadium w wysokości 3 000,00 złotych zostało wniesione w formie……*
6. *Integralną częścią oferty są wszystkie załączniki do oferty wymagane w specyfikacji jako niezbędne.*

Miejsce i data..... .....

Pieczątka i podpis osoby lub osób figurujących w rejestrach lub wpisie do ewidencji lub we właściwym pełnomocnictwie uprawnionych do zaciągania zobowiązań

Cyberbezpieczne Wodociągi

Dodatek nr 3 do SWZ
Wzór oświadczenia

(pieczęć adresowa firmy oferenta)

OŚWIADCZENIE

Przystępując do postępowania w sprawie udzielenia zamówienia na ***„Opracowanie dokumentacji i wykonanie audytów – obszar organizacyjny w ramach projektu „Cyberbezpieczne Wodociągi" realizowanego przez Przedsiębiorstwo Wodociągów i Kanalizacji Sp.z o.o. w Wołominie, w ramach Inwestycji C3.1.1 „Cyberbezpieczeństwo – CyberPL" – Cyberbezpieczne Wodociągi, finansowanego z Krajowego Planu Odbudowy i Zwiększania Odporności"***

ja (imię i nazwisko) .....

w imieniu reprezentowanej przeze mnie firmy.....

.....

oświadczam, że:

zapoznałem się ze specyfikacją warunków zamówienia i opisem przedmiotu zamówienia i nie wnoszę zastrzeżeń oraz uzyskałem konieczne informacje i wyjaśnienia do przygotowania oferty.
Upoważniamy Zamawiającego lub jego upoważnionych przedstawicieli do przeprowadzenia badań mających na celu sprawdzenie doświadczeń, dokumentów i przedstawionych informacji oraz do wyjaśnienia wszystkich aspektów zgłoszonej oferty.
Deklarujemy, że wszystkie oświadczenia i informacje zamieszczone w ofercie i załącznikach są aktualne i kompletne.

Miejsce i data..... Podpis.....

Podpis osoby lub osób figurujących w rejestrach lub wpisie do ewidencji lub we właściwym pełnomocnictwie uprawnionych do zaciągania zobowiązań

Cyberbezpieczne Wodociągi

Dodatek nr 4 do SWZ
Wzór oświadczenia o braku podstaw do wykluczenia

(pieczęć adresowa firmy oferenta)

OŚWIADCZENIE

o braku podstaw do wykluczenia z udziału w postępowaniu

Przystępując do postępowania o udzielenie zamówienia na:
„Opracowanie dokumentacji i wykonanie audytów – obszar organizacyjny w ramach projektu „Cyberbezpieczne Wodociągi" realizowanego przez Przedsiębiorstwo Wodociągów i Kanalizacji Sp.z o.o. w Wołominie, w ramach Inwestycji C3.1.1 „Cyberbezpieczeństwo – CyberPL" – Cyberbezpieczne Wodociągi, finansowanego z Krajowego Planu Odbudowy i Zwiększania Odporności"
ja (imię i nazwisko) .....

w imieniu reprezentowanej przeze mnie firmy.....

.....

oświadczam, że:
nie podlegamy wykluczeniu z postępowania na podstawie przesłanek zawartych w Dziale IV, Rozdziale X, Regulaminu udzielania przez Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o. z siedzibą w Wołominie zamówień nieobjętych ustawą z dnia 11 września 2019 r. Prawo Zamówień Publicznych – zatwierdzonego Uchwałą nr 4/2026 z dnia 23.02.2026 r.

Miejsce i data..... Podpis.....

Podpis osoby lub osób figurujących w rejestrach lub wpisie do ewidencji lub we właściwym pełnomocnictwie uprawnionych do zaciągania zobowiązań

Dodatek nr 5 do SWZ
Wzór umowy

(pieczęć adresowa firmy Wykonawcy)

UMOWA nr .....
(zwana dalej: ***umową)***
Zawarta w dniu ..... w **Wołominie** pomiędzy

Przedsiębiorstwem Wodociągów i Kanalizacji Sp. z o.o. z siedzibą w Wołominie, przy ulicy Granicznej 1, 05-200 Wołomin, wpisanym do rejestru przedsiębiorców Sądu Rejonowego dla m.st. Warszawy w Warszawie, XIV Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000002980, NIP 1250005499, posiadającym kapitał zakładowy 80 592 500,00 zł, reprezentowanym przez:
Wojciecha Jankowskiego – Prezesa Zarządu,
zwanym dalej ***Zamawiającym***

a
..... z siedzibą przy ....., wpisanym do ....., pod numerem ....., NIP ....., reprezentowanym przez:

.....
zwanym dalej **Wykonawcą,**

Na podstawie dokonanego przez Zamawiającego wyboru Oferty Wykonawcy w postępowaniu o udzielenie zamówienia, prowadzonym w trybie przetargu nieograniczonego w oparciu o postępowanie wewnętrznego „Regulaminu udzielania przez Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o. z siedzibą w Wołominie zamówień nieobjętych ustawą z dnia 11 września 2019 r. Prawo Zamówień Publicznych – zatwierdzonego Uchwałą nr 4/2026 z dnia 23.02.2026 r. została zawarta Umowa następującej treści:

§ 1
Przedmiot umowy

Przedmiotem niniejszej umowy jest:
1. Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)
Przedmiotem usługi jest opracowanie oraz wsparcie we wdrożeniu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) u Zamawiającego. Usługa ma charakter jednorazowy i kończy się przekazaniem odebraniem gotowej dokumentacji wraz ze wsparciem eksperckim w toku procesu wdrożeniowego.

Wykonawca opracowuje dokumentację SZBI obejmującą politykę bezpieczeństwa informacji oraz kluczowe polityki tematyczne dostosowane do specyfiki operatora wodociągowego — w szczególności dotyczące kontroli dostępu do systemów IT i OT, zarządzania incydentami bezpieczeństwa (w tym incydentami zgłaszanymi do właściwego CSIRT zgodnie z uoKSC), bezpieczeństwa pracy zdalnej i urządzeń mobilnych, zarządzania kopiami zapasowymi oraz

bezpieczeństwa relacji z dostawcami i wykonawcami zewnętrznymi. Liczba i szczegółowość opracowywanych dokumentów powinna wynika z analizy organizacji i powinna zostać uzgodniona z Zamawiającym przed przystąpieniem do właściwych prac. Wykonawca opracowuje dokumentację SZBI skoncentrowaną na kluczowych, praktycznych elementach możliwych do wdrożenia i utrzymania przez Zamawiającego. Zakres dokumentacji jest ograniczony do uzgodnionych obszarów i może nie obejmować wszystkich zabezpieczeń z Załącznika A normy ISO/IEC 27001 ma jednak pokrywać wymagania UoKSC.

W ramach usługi Wykonawca przeprowadzi wspólnie, w formie warsztatowej, z Zamawiającym wstępne szacowanie ryzyka obejmujące inwentaryzację kluczowych aktywów informacyjnych i systemów teleinformatycznych, identyfikację głównych zagrożeń istotnych dla operatora wodociągowego (w tym zagrożeń dla ciągłości dostaw wody i integralności systemów sterowania) oraz opracowanie uproszczonego Planu Postępowania z Ryzykiem wskazującego priorytety działań. Szacowanie ryzyka jest realizowane w ujęciu uproszczonym, ukierunkowanym na identyfikację kluczowych aktywów, zagrożeń i priorytetów postępowania z ryzykiem, z uwzględnieniem skali oraz kontekstu Zamawiającego. Metodyka pracy jest dostosowana do potrzeb projektu i może nie obejmować wszystkich elementów podejścia zgodnego z ISO/IEC 27005.W trakcie wdrożenia Wykonawca zapewnia wsparcie merytoryczne. Wsparcie obejmuje konsultacje dotyczące stosowania opracowanej dokumentacji oraz pomoc w przygotowaniu personelu do jej użytkowania.

Integralnym elementem usługi jest przeszkolenie kluczowego personelu Zamawiającego obejmujące omówienie struktury systemu zarządzania, sposobu stosowania kluczowych polityk i procedur oraz podstaw prowadzenia przeglądu dokumentacji. Szkolenie ma na celu wyposażenie wyznaczonych pracowników w wiedzę niezbędną do samodzielnego posługiwania się przekazaną dokumentacją.

Dokumentacja SZBI jest opracowywana z uwzględnieniem wymagań ustawy o krajowym systemie cyberbezpieczeństwa, Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności oraz normy PN-EN ISO/IEC 27001:2023 jako punktu odniesienia dla dobrych praktyk w zakresie zarządzania bezpieczeństwem informacji.

Zamawiający oczekuje, że rezultatem usługi będzie przekazanie dokumentacji SZBI dostosowanej do skali i specyfiki Zamawiającego, wraz z rekomendacjami dotyczącymi dalszego podnoszenia poziomu bezpieczeństwa.

2. Opracowanie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP) dla STI

Przedmiotem usługi jest pomoc w opracowaniu oraz wsparcie we wdrożeniu Planów Ciągłości Działania (BCP) i Planów Odtwarzania po Awarii (DRP) dla systemów teleinformatycznych (STI) Zamawiającego. Plany będą stanowić dokumenty operacyjne określające konkretne działania, sekwencje kroków, role personelu i zasoby niezbędne do utrzymania lub przywrócenia sprawności krytycznych systemów IT w przypadku awarii lub zakłócenia. Usługa jest realizowana jako projekt o zdefiniowanym zakresie i terminie zakończenia.

Etap wstępny będzie obejmował identyfikację systemów teleinformatycznych kluczowych dla utrzymania ciągłości usługi wodociągowej, przegląd istniejących rozwiązań w zakresie kopii zapasowych i redundancji IT oraz rozpoznanie kluczowych zależności między systemami IT a procesami operacyjnymi Zamawiającego. Na tej podstawie Wykonawca wspólnie z Zamawiającym wybierze dwa kluczowe, reprezentatywne systemy (przypadki wzorcowe), dla

których zostaną opracowane przykładowe plany BCP i DRP oraz ujednolicone procedury towarzyszące, co definiuje zamknięty zakres usługi.

Kluczowym elementem usługi jest przeprowadzenie warsztatowej analizy wpływu na działalność (BIA) wspólnie z wyznaczonymi przedstawicielami Zamawiającego. Warsztaty służą wyznaczeniu dla dwóch wybranych systemów (przypadków wzorcowych): orientacyjnego Docelowego Czasu Odtworzenia (RTO), orientacyjnego Docelowego Punktu Odtworzenia (RPO) oraz priorytetu odtwarzania. Wyniki BIA będą dokumentowane i będą stanowiły bezpośrednią podstawę projektowania treści planów. Jeżeli w toku warsztatów nie będzie możliwe uzyskanie danych niezbędnych dla konkretnego systemu, Wykonawca odnotuje przyjęte założenia zastępcze i uzgodni z Zamawiającym sposób postępowania — np. zawężenie zakresu planu lub opisanie ograniczeń przyjętych przy jego opracowaniu.

Na podstawie wyników analizy BIA Wykonawca wspólnie z Zamawiającym opracowuje dla dwóch wybranych systemów (w ujęciu wzorcowym) Plan Ciągłości Działania (BCP) określający procedury postępowania w trakcie trwania zakłócenia — w tym tryb pracy awaryjnej, zastępcze sposoby realizacji funkcji systemu oraz zasady komunikacji wewnętrznej i eskalacji — oraz Plan Odtwarzania po Awarii (DRP) określający krok po kroku procedury technicznego przywrócenia sprawności systemu po zakończeniu zakłócenia, wymagane zasoby i narzędzia, role techniczne personelu oraz kryteria zakończenia procesu odtwarzania. Uzupełnieniem planów są ujednolicone procedury zarządzania kopiami zapasowymi, zapewniające spójność z parametrami RPO przyjętymi w analizie BIA.

W toku wdrożenia Wykonawca przeprowadzi szkolenie dla wyznaczonego przez Zamawiającego personelu, obejmujące omówienie struktury i logiki opracowanych planów, sposobu ich stosowania w praktyce oraz zasad ich aktualizacji. Ponadto Wykonawca wspólnie z Zamawiającym przeprowadza jedno ćwiczenie stołowe (table-top) dla jednego z opracowanych planów, demonstrując praktycznie przebieg testu i sposób dokumentowania jego wyników. Ćwiczenie to ma charakter instruktażowy i stanowi wzorzec dla samodzielnego przeprowadzania kolejnych testów przez Zamawiającego. Regularne testy pozostałych planów będą realizowane przez Zamawiającego we własnym zakresie po zakończeniu usługi.

Plany są opracowywane z uwzględnieniem wymagań ustawy o krajowym systemie cyberbezpieczeństwa, Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności oraz normy PN-EN ISO 22301 jako punktu odniesienia dla dobrych praktyk w zakresie planowania ciągłości działania.

Rezultatem usługi jest przekazanie Zamawiającemu zamkniętego zestawu planów BCP i DRP dla uzgodnionych systemów STI, gotowych do bezpośredniego stosowania przez personel Zamawiającego, wraz z rekomendacjami dotyczącymi dalszego utrzymania i rozwijania dokumentacji.

3. Audyt KRI, Audyt SZBI, Audyt ciągłości działania

3.1. Audyt KRI

Realizacja audytu bezpieczeństwa informacji będzie prowadzona jako audyt zgodności systemów organizacyjnych oraz technicznych z obowiązującymi wymaganiami Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej.

Audyt zostanie przeprowadzony w oparciu o metodykę audytową określoną w normie PN-EN ISO 19011:2018, stanowiącej międzynarodowy standard w zakresie planowania, realizacji, dokumentowania oraz raportowania audytów systemów zarządzania. W toku realizacji czynności audytowych zastosowane zostaną zasady niezależności, bezstronności, podejścia opartego na dowodach oraz podejścia systemowego, umożliwiające kompleksową ocenę dojrzałości organizacyjnej oraz skuteczności wdrożonych mechanizmów bezpieczeństwa informacji.

Jednocześnie zakres merytoryczny audytu zostanie ukształtowany w oparciu o wybrane wymagania i dobre praktyki wynikające z normy PN-EN ISO/IEC 27001:2023, w szczególności w obszarach zarządzania ryzykiem bezpieczeństwa informacji, organizacyjnych i technicznych środków ochrony informacji, zarządzania dostępem do zasobów teleinformatycznych, monitorowania zdarzeń bezpieczeństwa, realizacji kopii zapasowych oraz zapewnienia ciągłości działania systemów informatycznych. Norma ISO/IEC 27001 będzie stanowiła referencyjny punkt odniesienia dla oceny adekwatności i proporcjonalności stosowanych zabezpieczeń w relacji do zidentyfikowanych zagrożeń i poziomu ryzyka.

Audyt zostanie zrealizowany w formie audytu na miejscu (on-site) w siedzibie Zamawiającego. Zakres prac obejmować będzie przeprowadzenie szczegółowej analizy dokumentacji systemowej i proceduralnej, w tym polityk bezpieczeństwa informacji, procedur zarządzania incydentami, analiz ryzyka, rejestrów uprawnień, ewidencji aktywów oraz dokumentacji technicznej środowiska teleinformatycznego. Uzupełnieniem analizy dokumentacyjnej będą wywiady audytowe z odpowiednimi osobami, a także wyrywkowa weryfikacja wybranych elementów infrastruktury i stanowisk pracy pod kątem zgodności z przyjętymi regulacjami oraz dobrymi praktykami bezpieczeństwa IT.

Przeprowadzone czynności audytowe umożliwią dokonanie kompleksowej oceny stopnia spełnienia minimalnych wymagań wynikających z Krajowych Ram Interoperacyjności.

Efektem audytu będzie sporządzenie raportu końcowego zawierającego syntetyczną ocenę poziomu zgodności, identyfikację stwierdzonych niezgodności, luk i obszarów podwyższonego ryzyka, a także zestaw rekomendacji ukierunkowanych na podniesienie poziomu bezpieczeństwa informacji oraz zapewnienie pełnej zgodności regulacyjnej. Raport stanowić będzie formalny dokument potwierdzający realizację obowiązków audytowych wynikających z przepisów prawa oraz podstawę do planowania dalszych działań organizacyjnych i technicznych w obszarze cyberbezpieczeństwa.

Audyt zostanie przeprowadzony przez zespół audytorów posiadających kwalifikacje i doświadczenie w zakresie audytów bezpieczeństwa informacji, stosowania metodyki ISO 19011 oraz wdrażania i oceny systemów zarządzania bezpieczeństwem informacji zgodnych z normą ISO/IEC 27001, co zapewni wysoką jakość merytoryczną oraz wiarygodność uzyskanych wyników.

3.2. Audyt SZBI wg ISO27001

Realizacja audytu bezpieczeństwa informacji będzie prowadzona jako audyt zgodności systemów organizacyjnych oraz technicznych z obowiązującymi wymaganiami Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej.

Audyt zostanie przeprowadzony w oparciu o metodykę audytową określoną w normie PN-EN ISO 19011:2018, stanowiącej międzynarodowy standard w zakresie planowania, realizacji,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

dokumentowania oraz raportowania audytów systemów zarządzania. W toku realizacji czynności audytowych zastosowane zostaną zasady niezależności, bezstronności, podejścia opartego na dowodach oraz podejścia systemowego, umożliwiające kompleksową ocenę dojrzałości organizacyjnej oraz skuteczności wdrożonych mechanizmów bezpieczeństwa informacji.

Jednocześnie zakres merytoryczny audytu zostanie ukształtowany w oparciu o wybrane wymagania i dobre praktyki wynikające z normy PN-EN ISO/IEC 27001:2023, w szczególności w obszarach zarządzania ryzykiem bezpieczeństwa informacji, organizacyjnych i technicznych środków ochrony informacji, zarządzania dostępem do zasobów teleinformatycznych, monitorowania zdarzeń bezpieczeństwa, realizacji kopii zapasowych oraz zapewnienia ciągłości działania systemów informatycznych.

Norma ISO/IEC 27001 będzie stanowiła referencyjny punkt odniesienia dla oceny adekwatności i proporcjonalności stosowanych zabezpieczeń w relacji do zidentyfikowanych zagrożeń i poziomu ryzyka.

Audyt zostanie zrealizowany w formie audytu na miejscu (on-site) w siedzibie Zamawiającego. Zakres prac obejmować będzie przeprowadzenie szczegółowej analizy dokumentacji systemowej i proceduralnej, w tym polityk bezpieczeństwa informacji, procedur zarządzania incydentami, analiz ryzyka, rejestrów uprawnień, ewidencji aktywów oraz dokumentacji technicznej środowiska teleinformatycznego. Uzupełnieniem analizy dokumentacyjnej będą wywiady audytowe z odpowiednimi osobami, a także wyrywkowa weryfikacja wybranych elementów infrastruktury i stanowisk pracy pod kątem zgodności z przyjętymi regulacjami oraz dobrymi praktykami bezpieczeństwa IT.

Przeprowadzone czynności audytowe umożliwią dokonanie kompleksowej oceny stopnia spełnienia minimalnych wymagań wynikających z Krajowych Ram Interoperacyjności.

Efektem audytu będzie sporządzenie raportu końcowego zawierającego syntetyczną ocenę poziomu zgodności, identyfikację stwierdzonych niezgodności, luk i obszarów podwyższonego ryzyka, a także zestaw rekomendacji ukierunkowanych na podniesienie poziomu bezpieczeństwa informacji oraz zapewnienie pełnej zgodności regulacyjnej. Raport stanowić będzie formalny dokument potwierdzający realizację obowiązków audytowych wynikających z przepisów prawa oraz podstawę do planowania dalszych działań organizacyjnych i technicznych w obszarze cyberbezpieczeństwa.

Audyt zostanie przeprowadzony przez zespół audytorów posiadających kwalifikacje i doświadczenie w zakresie audytów bezpieczeństwa informacji, stosowania metodyki ISO 19011 oraz wdrażania i oceny systemów zarządzania bezpieczeństwem informacji zgodnych z normą ISO/IEC 27001, co zapewni wysoką jakość merytoryczną oraz wiarygodność uzyskanych wyników.

3.3. Audyt SZCD STI wg ISO 22301

Przegląd Systemu Zarządzania Ciągłością Działania (SZCD) dla Systemów Teleinformatycznych i Infrastruktury (STI) zgodnie z ISO 22301:2019

Przedmiotem zamówienia jest wykonanie przeglądu Systemu Zarządzania Ciągłością Działania (SZCD) wdrożonego w organizacji Zamawiającego, w zakresie systemów teleinformatycznych (IT), systemów technologicznych (OT/SCADA) oraz usług świadczonych z wykorzystaniem infrastruktury teleinformatycznej (STI), pod kątem zgodności z wymaganiami normy ISO

22301:2019. Przegląd nie stanowi audytu certyfikacyjnego, audytu technicznego, oceny bezpieczeństwa systemów IT i OT.

Celem realizacji zamówienia jest:

1. Ocena zgodności SZCD z wymaganiami normy ISO 22301:2019;
2. Weryfikacja skuteczności przyjętych rozwiązań organizacyjnych, technicznych i proceduralnych;
3. Identyfikacja luk i obszarów wymagających doskonalenia;
4. Przygotowanie rekomendacji działań usprawniających.

Zamawiający wymaga, by ocena zgodności objęła wszystkie obszary normy ISO 22301:2019 (rozdziały 4–10). Zamawiający wymaga, by w ramach prac Wykonawca dokonał przeglądu dokumentacji obejmującej kontekst organizacji (w tym przynajmniej: zakres funkcjonowania SZCD, kontekst wewnętrzny i zewnętrzny, identyfikacja stron zainteresowanych, wymagania prawne i regulacyjne, zgodność zakresu SZCD z działalnością przedsiębiorstwa) oraz dokumentacji SZCD udostępnionej przez Zamawiającego.

Przegląd dokumentacji SZCD obejmie w szczególności: Politykę Ciągłości Działania, cele SZCD oraz przypisanie ról, odpowiedzialności i uprawnień; zakres systemu; analizę wpływu na działalność (BIA) wraz z parametrami czasowymi (MTPD, RTO); ocenę ryzyka zakłóceń działań krytycznych, a także ryzyka i szanse odnoszące się do samego systemu zarządzania; przyjęte strategie i rozwiązania ciągłości działania wraz z wymaganiami dotyczącymi zasobów oraz parametrami RTO, RPO i MBCO; plany ciągłości działania (BCP) i plany odtworzeniowe IT (DRP); strukturę reagowania oraz procedury ostrzegania i komunikacji w sytuacji zakłócenia; procedury testowania i ćwiczeń; procedury przeglądów i doskonalenia. Przeglądowi podlegają również zapisy potwierdzające funkcjonowanie systemu, w tym dowody kompetencji i świadomości personelu, wskaźniki i wyniki monitorowania skuteczności SZCD, zapisy z audytów wewnętrznych i przeglądów zarządzania oraz rejestr niezgodności i działań korygujących. Zamawiający udostępni także rejestry usług krytycznych, zasobów ryzyk oraz dokumentację dotyczącą dostawców usług krytycznych).

Wykonawca wykona także przegląd infrastruktury IT i OT, w tym: zakresie niezbędnym do potwierdzenia spełnienia wymagań ISO 22301, rozumianym jako przegląd istnienia i skuteczności mechanizmów istotnych dla ciągłości działania.

Przegląd obejmie:

1. obszar IT: serwery, macierze dyskowe, systemy kopii zapasowych, środowiska wirtualne, sieć LAN/WAN, systemy bezpieczeństwa, Active Directory, usługi chmurowe, system ERP, system bilingowy, GIS.
2. obszar OT: systemy SCADA; sterowniki PLC; systemy telemetryczne; systemy monitoringu sieci; systemy sterowania pompowniami; systemy sterowania stacjami uzdatniania; systemy sterowania oczyszczalniami.

W czasie realizacji przeglądu Wykonawca dokona analizę dokumentacji Zamawiającego, przeprowadzi wywiady z przedstawicielami Zamawiającego; zweryfikuje konfiguracje wybranych systemów (w zakresie niezbędnym dla potwierdzenia spełnienia wymagań ISO 22301), zbierze dowody na funkcjonowanie SZCD, przeprowadzi analizę wyników ćwiczeń i

testów. Przegląd odbędzie się on-site, wraz z wizją lokalną w wybranych obiektach Zamawiającego.

Po zakończonym przeglądzie, Wykonawca dostarczy raport, zawierający ocenę zgodności z ISO 22301, wykaz niezgodności, obserwacji oraz ryzyk, a także rekomendacje działań doskonalących.

Wykonawca wskaże dla każdej zidentyfikowanej niezgodności opis, poziom ryzyka, rekomendowane działania oraz priorytet realizacji.

Zamawiający wymaga, by raport został zaprezentowany na spotkaniu zamykającym z kierownictwem Zamawiającego.

Osoby skierowane do realizacji zamówienia powinny posiadać doświadczenie w:

1. audytowaniu lub wdrażaniu systemów zgodnych z ISO 22301;
2. ocenie środowisk IT oraz OT/SCADA;
3. prowadzeniu audytów systemów zarządzania.

4. Testy bezpieczeństwa

4.1. Testy bezpieczeństwa infrastruktury sieciowej IT/OT/ICS/IIoT

Wykonawca zobowiązany jest do przeprowadzenia testu penetracyjnego infrastruktury Zamawiającego w metodyce gray-box, w taki sposób, aby poprzez próbę przełamania zabezpieczeń umożliwić identyfikację ryzyk oraz potencjalnych konsekwencji ewentualnego włamania. Test penetracyjny musi być wykonywany zarówno manualnie, jak i automatycznie, z wykorzystaniem specjalistycznych narzędzi oraz własnych skryptów przygotowanych na podstawie wiedzy i doświadczeń Wykonawcy. Testy muszą zostać przeprowadzone w oparciu o metodologię OSSTMM (Open Source Security Testing Methodology Manual) lub równoważną, przy zapewnieniu co najmniej równoważnego zakresu i poziomu szczegółowości.

Metoda równoważna musi zapewniać co najmniej ten sam poziom jakości, pokrycia i rygoru testów. Dotyczy to poniższych kluczowych kryteriów:

1) metodyka działania powinna jasno definiować:

   a) etapy testów (planowanie, rekonesans, testy właściwe, raportowanie),
   b) podejście do identyfikacji podatności,
   c) sposób weryfikacji i potwierdzania wyników (brak „false positives").

2) poziom szczegółowości:

   a) testy nie mogą być powierzchowne (np. tylko skan automatyczny),
   b) wymagane są techniki manualne i analiza ekspercka,
   c) opis podatności musi zawierać dowody, wpływ i rekomendacje.

3) powtarzalność i mierzalność:

   a) metodologia powinna umożliwiać odtworzenie testów,
   b) metodologia powinna zawierać sposób oceny ryzyka lub klasyfikacji podatności.

Wykonawca zobowiązany jest do realizacji testów penetracyjnych infrastruktury w co najmniej dwóch fazach: zewnętrznej i wewnętrznej. Wewnętrzna ocena bezpieczeństwa infrastruktury

powinna umożliwiać identyfikację wewnętrznych ryzyk występujących w organizacji. Testy wewnętrzne mogą być realizowane zdalnie.

Test penetracyjny infrastruktury musi umożliwić identyfikację istniejących podatności oraz dostarczyć praktyczne dowody czy podatności te mogą zostać wykorzystane.

W ramach realizacji zamówienia Wykonawca zobowiązany jest do wykonania co najmniej następujących czynności:

1) Skanowanie sieci.
2) Weryfikacja domyślnych haseł w usługach umożliwiających logowanie.
3) Wykrycie możliwości przechwycenia haseł w sieci oraz weryfikacja pod kątem możliwości złamania haseł.
4) Testowanie bezpieczeństwa urządzeń drukujących.
5) Testowanie konfiguracji protokołów Secure Socket Layer (SSL) / Transport Layer Security (TLS). Sprawdzenie czy konfiguracja serwera nie zezwala na wykorzystanie starszych wersji protokołów TLS lub SSL oraz zweryfikowanie, czy nie jest możliwe korzystanie ze słabych algorytmów szyfrowania, które potencjalnie można rozszyfrować.
6) Testowanie usług sieciowych (w szczególności FTP, SSH, Telnet, SMTP, POP3, SMB itp.).
7) Przeprowadzenie działań typu spoofing (ataku polegającego na fałszowaniu lub modyfikowaniu danych w celu przejęcia tożsamości lub podszywania się pod inną osobę, system lub urządzenie w celu oszustwa lub uzyskania nieautoryzowanego dostępu).
8) Weryfikacja możliwości uzyskania dostępu do współdzielonych zasobów.
9) Testowanie bezpieczeństwa sieci bezprzewodowych (WiFi) jeżeli występuje w lokalizacji.
10) Testowanie bezpieczeństwa baz danych w zakresie brute force i podatności
11) Identyfikacja podatności w usługach sieciowych i aplikacjach docelowych.
12) Wykorzystanie zidentyfikowanych podatności przy użyciu odpowiednich narzędzi, skryptów i metod, w zakresie uzgodnionym z Zamawiającym.

4.2. Testy bezpieczeństwa serwisów internetowych IT/OT/ICS

Testy bezpieczeństwa zostaną przeprowadzone w metodyce gray-box, tj. z ograniczoną wiedzą o systemie.

Test będzie realizowany zgodnie z uznanymi standardami branżowymi w zakresie testów bezpieczeństwa aplikacji i serwisów webowych, w szczególności:

1) OWASP Top 10,
2) OWASP Web Security Testing Guide

lub standardami równoważnymi obejmującymi wskazane kategorie podatności.

W ramach testów Wykonawca dokona weryfikacji podatności w szczególności w zakresie:

1) Injection – podatności związanych z wstrzyknięciami (np. SQL Injection, Command Injection),
2) Broken Authentication and Session Management – słabości mechanizmów uwierzytelniania oraz zarządzania sesją,
3) Cross-Site Scripting (XSS) – podatności na ataki typu XSS,

4) Insecure Direct Object References – nieautoryzowanego dostępu do zasobów poprzez manipulację identyfikatorami obiektów,
5) Security Misconfiguration – błędów konfiguracji bezpieczeństwa,
6) Sensitive Data Exposure – niewłaściwej ochrony danych wrażliwych,
7) Missing Function Level Access Control – błędów w kontroli dostępu do funkcji systemu,
8) Cross-Site Request Forgery (CSRF) – podatności na ataki CSRF,
9) Using Components with Known Vulnerabilities – wykorzystania komponentów zawierających znane podatności,
10) Unvalidated Redirects and Forwards – nieprawidłowej walidacji przekierowań.

Testy będą prowadzone z wykorzystaniem metod manualnych oraz narzędzi wspomagających, przy czym zautomatyzowane skanery podatności nie będą stanowiły jedynej metody badawczej.

1. Zasady bezpieczeństwa prowadzenia testów

Testy nie obejmują:

1) testów destrukcyjnych,
2) testów typu Denial of Service (DoS),
3) wprowadzania zmian konfiguracyjnych w środowisku Zamawiającego.

W przypadku wykrycia podatności o krytycznym poziomie ryzyka, Wykonawca zobowiązany jest do:

1) niezwłocznego poinformowania Zamawiającego,
2) udokumentowania podatności w sposób umożliwiający jej weryfikację,
3) czasowego wstrzymania dalszych testów bezpieczeństwa w zakresie mogącym wpływać na stabilność systemu.

Kontynuacja audytu nastąpi po podjęciu decyzji przez Zamawiającego dotyczącej dalszego sposobu prowadzenia testów.

2. Wyniki testów – raporty

Po zakończeniu testów Wykonawca przygotuje raporty z audytu bezpieczeństwa zawierający co najmniej:

1) opis metodyki przeprowadzonych testów,
2) wykaz zidentyfikowanych podatności,
3) klasyfikację podatności według poziomu ryzyka (np. CVSS Common Vulnerability Scoring System lub równoważnego standardu),
4) opis scenariusza wykorzystania podatności (proof-of-concept),
5) ocenę wpływu podatności na bezpieczeństwo systemu,
6) rekomendacje działań naprawczych.

Raporty zostaną przekazane w formie elektronicznej. Po przekazaniu raportów Wykonawca zobowiązuje się do nieprzechowywania danych po zakończeniu zamówienia.

§ 2

Termin realizacji umowy

Wykonawca zobowiązuje się zrealizować powierzone zadanie do dnia 30.11.2026 r.

§ 3

Wynagrodzenie

1. Wysokość wynagrodzenia za wykonanie „Przedmiotu Zamówienia", Strony ustalają na podstawie Oferty Wykonawcy.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

2. Za wykonanie przedmiotu umowy Wykonawcy przysługuje od Zamawiającego wynagrodzenie w wysokości:
Netto- ..... (słownie: ..... złotych) VAT – ..... zł
Brutto ..... zł (słownie: ..... złotych)
W tym:

Lp	Nazwa	wartość netto PLN	wartość VAT PLN	wartość brutto PLN
1	Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)			
2	Opracowanie planów ciągłości działania (BCP) i odtworzenia po awarii (DRP) dla STI			
3	Audyt zgodności KRI			
4	Audyt SZBI			
5	Audyt ciągłości działania			
6	Testy bezpieczeństwa infrastruktury sieciowej IT/OT/ICS /IIoT			
7	Testy bezpieczeństwa serwisów internetowych IT/OT /ICS			

3. Zamawiający dopuszcza płatności częściowe.
4. Płatności częściowe będą dopuszczalne w maksymalnie trzech transzach:
   a. Po odbiorze części I, na podstawie podpisanego przez strony protokołu odbioru częściowego – Wykonanie testów bezpieczeństwa infrastruktury sieciowej IT/OT/ICS/IIoT i testów bezpieczeństwa serwisów internetowych IT/OT/ICS.
   b. Po odbiorze części II, na podstawie podpisanego przez strony protokołu odbioru częściowego – Wykonanie Audytu KRI, Audytu SZBI, Audytu ciągłości działania.
   c. Po odbiorze końcowym, na podstawie podpisanego przez strony protokołu końcowego - Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), Opracowanie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP) dla STI.
5. Wypłata wynagrodzenia nastąpi w formie przelewu na rachunek Wykonawcy wskazany na fakturze VAT, w terminie do 30 dni od daty otrzymania prawidłowo wystawionej faktury VAT. Wykonawca zobowiązany jest każdorazowo podawać w treści wystawianej faktury VAT termin płatności. Wykonawca oświadcza, iż rachunek bankowy, na który Zamawiający zobowiązany będzie przelać wynagrodzenie, jest rachunkiem bankowym znajdującym się w elektronicznym wykazie podmiotów prowadzonych od 01.09.2019 r. przez Szefa Krajowej Administracji Skarbowej, o którym mowa w ustawie o podatku od towarów i usług.
6. W przypadku przedstawienia przez Wykonawcę nieprawidłowo – w rozumieniu umowy i/lub ustawy o VAT - wystawionej faktury VAT lub wskazania numeru rachunku nie widniejącego w elektronicznym wykazie, o którym mowa w ust. 5, Zamawiający ma prawo odmówić jej przyjęcia bez negatywnych dla siebie konsekwencji. W takim wypadku objęta fakturą należność nie będzie traktowana jako wymagalna i nie będzie

pociągać za sobą obciążenia Wykonawcy ewentualnymi odsetkami za opóźnienie w płatności.

7. Termin płatności o którym mowa w ust. 5 będzie przedłużany o czas niezbędny do usunięcia niezgodności lub wad.

§ 4

Poufność

1. Wykonawca zobowiązuje się do zachowania w tajemnicy wszelkich informacji, uzyskanych w związku ze świadczeniem na rzecz Zamawiającego, w szczególności zawierających jakiekolwiek dane osobowe, techniczne, operacyjne, administracyjne, ekonomiczno-prawne, korporacyjne, marketingowe, planistyczne, biznesowe, finansowe, danych dotyczących strategii biznesowych, zamierzeń i osiągnięć lub dotyczących stosowanych przez Wykonawcę urządzeń, technologii i oprogramowania, zwanych w dalszej części niniejszej Umowy **„Informacjami Poufnymi"**.
2. Obowiązek określony w ust. 1 niniejszego paragrafu odnosi się do wszelkich Informacji Poufnych otrzymanych lub uzyskanych bezpośrednio od Zamawiającego lub za pośrednictwem osób działających w jego imieniu, ustnie, pisemnie, drogą elektroniczną, bądź w innej formie, bez względu na rodzaj nośnika Informacji Poufnych, w tym również informacji uzyskanych przez Wykonawcę przed podjęciem współpracy pomiędzy stronami i podpisaniem niniejszej Umowy.
3. Wykonawca zobowiązuje się zapewnić z najwyższą starannością, wynikającą z zawodowego charakteru jego czynności, utrzymanie w tajemnicy Informacji Poufnych w okresie trwania niniejszej umowy oraz po jej rozwiązaniu lub wygaśnięciu.
4. W terminie 3 dni po zakończeniu współpracy między stronami oraz na każde żądanie Zamawiającego, Wykonawca ma obowiązek zwrócenia Zamawiającemu na własny koszt wszelkich informacji, dokumentów i materiałów, które uzyskał w związku i przy okazji świadczenia usług na rzecz Zamawiającego.
5. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane przez nie do odbioru, przekazywania, przechowywania i wykorzystywania Informacji Poufnych gwarantowały zabezpieczenie Informacji Poufnych przed dostępem osób trzecich nie upoważnionych do zapoznania się z nimi.

§ 5

Obowiązki Stron

1. Zamawiający zobowiązany jest do:
   1) Sprawnej i efektywnej koordynacji zamówienia, w tym uzgadniania wszelkich kwestii merytorycznych, mających wpływ na prawidłową realizację umowy.
   2) Sprawnego i terminowego przeprowadzenia procedury odbioru końcowego.
   3) Zapłaty Wykonawcy jego wynagrodzenia na zasadach i terminach określonych niniejszą umową.
2. Wykonawca zobowiązany jest do:
   1) Przedłożenia w terminie 10 dni roboczych od dnia zawarcia umowy do zatwierdzenia Zamawiającemu harmonogramu realizacji prac, obejmującego podział na etapy, terminy realizacji oraz planowane terminy odbiorów częściowych.
   2) Realizacji przedmiotu umowy z należytą starannością w sposób określony odpowiednimi przepisami prawa obowiązującymi w zakresie przedmiotu umowy, przez osoby posiadające odpowiednie kwalifikacje zawodowe i wymagane uprawnienia.

3) Bieżących i ścisłych kontaktów z Zamawiającym, polegających na uzgadnianiu wszystkich kwestii, mających wpływ na prawidłową realizację przedmiotu umowy.
4) niezwłocznego informowania Zamawiającego o wszelkich przeszkodach i trudnościach mogących wpłynąć na realizację niniejszej Umowy.
5) Uzyskanie zgody Zamawiającego na zatrudnienie Podwykonawcy.

3. Określone zakresy obowiązków Zamawiającego i Wykonawcy stanowią podstawę stwierdzenia wykonania, niewykonania lub nienależytego wykonania umowy oraz ustalenia następstw tego stwierdzenia, stosownie do postanowień umowy.

§ 6

Gwarancja

1. Wykonawca udziela 24 miesięcznej gwarancji na wykonany przedmiot zamówienia liczonej od protokolarnego, bezwarunkowego odebrania przedmiotu umowy.
2. W przypadku stwierdzenia przez Zamawiającego istnienia wad dokumentacji, Wykonawca zobowiązany jest do ich niezwłocznego usunięcia pod rygorem zastosowania kar umownych.
3. Wykonawca zobowiązany jest do niezwłocznego usunięcia wad dokumentacji w terminie nie później niż 14 dni od dnia doręczenia zawiadomienia o ujawnionych wadach. Termin usunięcia wad w uzasadnionych przypadkach może zostać wydłużony za pisemną zgodą Zamawiającego.
4. Wykonawca nie może odmówić usunięcia wad bez względu na związane z tym koszty.
5. W razie nieusunięcia wad w wyznaczonym terminie Zamawiający może zlecić ich usunięcie innym podmiotom na koszt i ryzyko Wykonawcy. Zamawiający powiadomi pisemnie Wykonawcę o skorzystaniu z powyższego uprawnienia. Wykonawca zobowiązany jest do zapłaty wynagrodzenia za wykonanie zastępcze w terminie 7 dni od daty wezwania go przez Zamawiającego.
6. W ramach gwarancji Wykonawca zobowiązuje się do przeglądu i aktualizacji dokumentacji w zakresie wynikającym z wdrożenia, wsparcia Zamawiającego w zakresie funkcjonowania dokumentacji, udzielania konsultacji dotyczących stosowania procedur będących przedmiotem niniejszej umowy.
7. W okresie obowiązywania umowy, jak i po jej rozwiązaniu lub po wygaśnięciu umowy, Wykonawca jest i będzie odpowiedzialny wobec Zamawiającego na zasadach uregulowanych w kodeksie cywilnym za wszelkie szkody jak i utracone korzyści (m.in. wydatki i koszty związane z postępowaniami sądowymi, administracyjnymi lub egzekucyjnymi) oraz roszczenia osób trzecich w przypadku, gdy będą one wynikać z wad przedmiotu umowy lub nie dołożenia należytej staranności przez Wykonawcę lub jego Podwykonawcę przy wykonaniu przedmiotu umowy.

§ 7

Kary umowne

1. W razie opóźnienia w wykonaniu przedmiotu umowy powstałego w skutek okoliczności, za które ponosi odpowiedzialność Wykonawca, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 0,5% wartości brutto określonej w § 3 ust. 2.
2. Wykonawca zapłaci Zamawiającemu karę umowną za odstąpienie od umowy przez którąkolwiek ze stron, z przyczyn, za które odpowiedzialność ponosi Wykonawca, w wysokości 10 % wynagrodzenia netto za cały przedmiot Umowy.
3. Zamawiający zapłaci Wykonawcy karę umowną za odstąpienie od umowy przez którąkolwiek ze stron, z przyczyn, za które odpowiedzialność ponosi Zamawiający, w wysokości 10 % wynagrodzenia netto za przedmiot Umowy.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

4. Wykonawca zapłaci Zamawiającemu karę umowną za naruszenie nakazu zachowania w tajemnicy informacji poufnych, o którym mowa w § 4 Umowy, w wysokości 50 % wynagrodzenia netto za cały przedmiot Umowy.
5. Wykonawca zapłaci Zamawiającemu karę umowną w przypadku niewykonania lub nienależytego wykonania przedmiotu umowy w czasie jej trwania w wysokości 2 000,00 zł brutto za każde naruszenie przez Wykonawcę zobowiązań wynikających z niniejszej umowy z wyłączeniem naruszeń.
6. Kary umowne mogą być potrącane z wynagrodzenia Wykonawcy, na co ten wyraża zgodę.
7. Strony zgodnie postanawiają, że zapłata kary umownej nastąpi w terminie 7 dni od daty wystąpienia z żądaniem zapłacenia kary przez każdą ze stron.
8. Strony zastrzegają sobie prawo do dochodzenia odszkodowania uzupełniającego przenoszącego wysokość kar umownych do wysokości rzeczywiście poniesionej szkody.

§ 8

Zmiany w umowie

1. W przypadkach przewidzianych w umowie dopuszcza się wprowadzenie istotnych zmian treści umowy za zgodą Zamawiającego.
2. Zmiany przewidziane w umowie mogą być inicjowane przez Zamawiającego lub przez Wykonawcę.
3. Zmiany, o których mowa w ust. 1 mogą dotyczyć:
   1) zmiany jakości lub innych parametrów charakterystycznych dla objętego proponowaną zmianą elementu przedmiotu umowy,
   2) zmiany zakresu rzeczowego przedmiotu zamówienia.
   3) zmiany terminów określonych w § 2 umowy,
   4) zmiany wynagrodzenia Wykonawcy (w tym podatku VAT),
4. Zmiany, o których mowa w ust. 3 mogą zostać dokonane, jeżeli zachodzą i są ich uzasadnieniem niżej wymienione okoliczności:
   1) zmiany obowiązujących przepisów,
   2) zmiany terminu w zakresie jego wydłużenia przy uzgodnieniu warunków finansowych i terminowych zaakceptowanych przez Strony,
   3) podniesienie wydajności przedmiotu umowy lub jego elementów,
   4) wystąpienia okoliczności, których strony umowy nie były w stanie przewidzieć, pomimo zachowania należytej staranności, w tym ograniczeniami o charakterze globalnym jak i lokalnym.
   5) opóźnienia, utrudnienia, zawieszenia prac powstałe w wyniku:
      a) niekorzystnych warunków atmosferycznych uniemożliwiających wykonanie prac (np. burze, ulewne deszcze, silne wiatry),
      b) przyczyn leżących po stronie Zamawiającego,
      c) działania siły wyższej (np. klęski żywiołowe, strajki generalne lub lokalne) mające bezpośredni wpływ na terminowość wykonania przedmiotu umowy,
      d) wystąpienia okoliczności, których strony umowy nie były w stanie przewidzieć, pomimo zachowania należytej staranności.
5. Zakazuje się zmiany umowy, jeżeli zmiana jest wymuszona uchybieniem czy naruszeniem umowy przez Wykonawcę. W takim przypadku koszty dodatkowe związane z takimi zmianami ponosi Wykonawca.
6. Dokonanie zmian umowy wymaga formy pisemnej pod rygorem nieważności.

§ 9

Zabezpieczenie należytego wykonania Umowy

1. Wykonawca wnosi zabezpieczenie należytego wykonania umowy w wysokości 5 % wynagrodzenia brutto tj. ..... zł
2. Zabezpieczenie należytego wykonania umowy zostanie wniesione w formie.....
3. Zamawiający zwróci 100% zabezpieczenia w nominalnej kwocie na pisemny wniosek Wykonawcy w terminie 30 dni od dnia wykonania umowy i uznania przez Zamawiającego za należycie wykonane.

§ 10

Nadzór

1. Nadzór nad prawidłową realizacją umowy ze strony Zamawiającego, będzie pełnił: .....
2. Nadzór nad prawidłową realizacją umowy ze strony Wykonawcy, będzie pełnił: .....

§ 11

Spory

1. Strony będą dążyły do polubownego załatwienia sporów mogących powstać w związku z realizacją Umowy.
2. W razie powstania sporu na tle wykonania niniejszej Umowy strony są zobowiązane przede wszystkim do wyczerpania drogi postępowania reklamacyjnego.
3. Reklamację wykonuje się poprzez skierowanie drugiej Stronie konkretnego roszczenia na piśmie.
4. Strona, do której wpłynęło roszczenie ma obowiązek do pisemnego ustosunkowania się do zgłoszonego roszczenia w terminie 7 dni roboczych od daty zgłoszenia.
5. Wszelkie spory wynikające z niniejszej umowy rozstrzygane będą przez sąd powszechny właściwy miejscowo dla Zamawiającego.

§ 12

Przepisy końcowe

1. Strony zobowiązują się wzajemnie do zawiadamiania drugiej Strony o każdorazowej zmianie adresu wskazanego w niniejszej umowie. Doręczenie pod adres wskazany przez Stronę, w przypadku odesłania zwrotnego przez pocztę przesyłki wysłanej na podany adres uważa się za skuteczne z upływem siódmego dnia, licząc od dnia następującego po dniu wysłania, jeżeli przesyłka nie została podjęta przez adresata, bez względu na przyczynę niepodjęcia.

   Adresy do doręczeń:
   Wykonawcy: ul. .....
   Zamawiającego: ul. Graniczna 1, 05-200 Wołomin
2. Sprawy sporne wynikłe z realizacji niniejszej umowy, których Strony nie rozwiążą polubownie, rozstrzygać będzie sąd właściwy miejscowo dla siedziby Zamawiającego.
3. W sprawach nieuregulowanych postanowieniami niniejszej Umowy, mają zastosowanie przepisy kodeksu cywilnego.
4. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

5. Umowę sporządzono w 2 jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Sporządziła: Urszula Papiór
Dział Inwestycji i Zamówień

WYKONAWCA ZAMAWIAJĄCY

Cyberbezpieczne Wodociągi

Dodatek nr 6 do SW

Wzór upoważnienia

(pieczęć adresowa firmy oferenta)

UPOWAŻNIENIE

Nazwa: .....
Siedziba: .....
Adres: .....
Telefony: .....
Miejsce rejestracji lub wpisu do ewidencji: .....
Upoważnionym przedstawicielem do uczestnictwa w przetargu, podpisywania oferty oraz innych dokumentów związanych z postępowaniem w sprawie udzielenia zamówienia na ***„Opracowanie dokumentacji i wykonanie audytów – obszar organizacyjny w ramach projektu „Cyberbezpieczne Wodociągi" realizowanego przez Przedsiębiorstwo Wodociągów i Kanalizacji Sp.z o.o. w Wołominie, w ramach Inwestycji C3.1.1 „Cyberbezpieczeństwo – CyberPL" – Cyberbezpieczne Wodociągi, finansowanego z Krajowego Planu Odbudowy i Zwiększania Odporności"***
i podejmowania decyzji w imieniu firmy jest:

.....

.....

.....

Miejsce i data..... Podpis.....

Podpis osoby lub osób figurujących w rejestrach lub wpisie do ewidencji lub we właściwym pełnomocnictwie uprawnionych do zaciągania zobowiązań

Cyberbezpieczne Wodociągi

Dodatek nr 7 do SWZ
Lista podmiotów – grupa kapitałowa

Lista podmiotów należących do tej samej grupy kapitałowej/informacja o tym, że wykonawca nie należy do grupy kapitałowej*.

WYKONAWCA:

Lp.		Nazwa(y) Wykonawcy(ów)	Adres(y) Wykonawcy(ów)
1.			
2.			

Przystępując do postępowania w sprawie udzielenia zamówienia na ***„Opracowanie dokumentacji i wykonanie audytów – obszar organizacyjny w ramach projektu „Cyberbezpieczne Wodociągi" realizowanego przez Przedsiębiorstwo Wodociągów i Kanalizacji Sp.z o.o. w Wołominie, w ramach Inwestycji C3.1.1 „Cyberbezpieczeństwo – CyberPL" – Cyberbezpieczne Wodociągi, finansowanego z Krajowego Planu Odbudowy i Zwiększania Odporności"***

1. **składamy listę podmiotów**, razem z którymi należymy do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. O ochronie konkurencji i konsumentów (Dz. U. z 2019 r. poz. 369).

Lp.	Nazwa podmiotu	Adres podmiotu
1		
2		
3		
....		

.....
(miejscowość, data)

.....
podpis osoby uprawnionej do reprezentowania wykonawcy

2. **informujemy, że nie należymy do grupy kapitałowej**, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U z 2019 r. poz. 369).

.....
(miejscowość, data)

.....
podpis osoby uprawnionej do reprezentowania wykonawcy

** UWAGA: - należy wypełnić pkt. 1 lub pkt. 2*

Dodatek nr 8 do SWZ
Klauzula Informacyjna

KLAUZULA INFORMACYJNA

Informacja o przetwarzaniu danych osobowych na podstawie 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 (dalej: RODO) Uprzejmie informujemy, że:

1) Administratorem Pani/Pana danych osobowych jest Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o. z siedzibą w Wołominie przy ul. Granicznej 1.
2) Dane kontaktowe w sprawach związanych bezpośrednio z przetwarzaniem danych osobowych:
   - adres korespondencji: Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o. o. ul. Graniczna 1, 05-200 Wołomin,
   - adres e-mail: iod@pwik.wolomin.pl.
3) Pani/Pana dane osobowe przetwarzane będą w celu przygotowania i przeprowadzenia postępowania o udzielenie zamówienia publicznego/realizacji umowy zawartej w wyniku przeprowadzenia postępowania o udzielenie zamówienia na podstawie przepisów ustawy Prawo zamówień publicznych oraz Regulaminu udzielania przez Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o. z siedzibą w Wołominie zamówień nieobjętych ustawą z dnia 11 września 2019 r. Prawo Zamówień Publicznych" – zatwierdzonego Uchwałą nr 4/2026 z dnia 23.02.2026 r., a także celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora;
4) Przetwarzanie danych osobowych obejmuje zakres danych podanych w formularzu ofertowym.
5) Pani/Pana dane osobowe mogą zostać powierzone następującym podmiotom: dostawcom systemów informatycznych, z którymi współpracuje Administrator, w celu utrzymania ciągłości oraz poprawności działania systemów; podmiotom prowadzącym działalność pocztową lub kurierską w celu dostarczenia korespondencji; upoważnionym z mocy prawa podmiotom na udokumentowany wniosek.
6) Dane osobowe nie będą przekazywane do państwa trzeciego ani do organizacji międzynarodowych.
7) Pani/Pana dane osobowe będą przechowywane:
   a) w okresie przygotowania i przeprowadzenia postępowania o udzielenie zamówienia – przez ten okres;
   b) w okresie realizacji umowy zawartej w wyniku przeprowadzenia postępowania o udzielenie zamówienia na podstawie przepisów ustawy Prawo zamówień publicznych lub Regulaminu udzielania przez Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o. z siedzibą w Wołominie zamówień nieobjętych ustawą z dnia 11 września 2019 r. Prawo Zamówień Publicznych" – zatwierdzonego Uchwałą nr 4/2026 z dnia 23.02.2026 r. – przez ten okres;
   c) w okresie po zakończeniu realizacji umowy, o której mowa w lit. b – przez okres, w którym administrator będzie realizował cele wynikające z prawnie uzasadnionych interesów realizowanych przez administratora, które są związane przedmiotowo z umową, o której mowa w lit. b lub obowiązkami wynikającymi z przepisów prawa powszechnie obowiązującego takich jak: przepisy podatkowe, ubezpieczeń majątkowych, dochodzenie odszkodowań i likwidacji szkód, ochrony praw autorskich, ubezpieczeń społecznych, o zasobie archiwalnym.
8) Posiada Pani/Pan prawo dostępu do treści swoich danych osobowych oraz prawo do ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych na zasadach określonych w przepisach o ochronie danych osobowych, w tym w unijnym Rozporządzeniu o Ochronie Danych Osobowych 2016/679 (RODO), prawo wniesienia sprzeciwu.
9) Ma Pani/Pan prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem (jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a)),
10) Ma Pani/Pan prawo w chwili, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych narusza przepisy o ochronie danych osobowych wniesienia skargi do organu nadzorczego zgodnie z art. 77 RODO, którym jest Prezes Urzędu Ochrony Danych Osobowych.
11) Podanie przez Panią/Pana danych osobowych jest dobrowolne, niemniej jest również warunkiem uczestnictwa Pani/Pana w procesie udzielenia zamówienia. Konsekwencją niepodania danych osobowych będzie brak możliwości udziału w postępowaniu o udzielenie zamówienia.
12) Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

4

Cyberbezpieczne Wodociągi

Dodatek nr 9 do SWZ

OŚWIADCZENIE WYKONAWCY

WYKLUCZENIE Z POSTĘPOWANIA NA PODSTAWIE ART. 7 UST. 1 USTAWY Z DNIA 13 KWIETNIA 2022 r. O SZCZEGÓLNYCH ROZWIĄZANIACH W ZAKRESIE PRZECIWDZIAŁANIA WSPIERANIU AGRESJI NA UKRAINĘ ORAZ SŁUŻĄCYCH OCHRONIE BEZPIECZEŃSTWA NARODOWEGO (Dz. U. 2025 poz. 514)

Przystępując do postępowania o udzielenie zamówienia na:

„Opracowanie dokumentacji i wykonanie audytów – obszar organizacyjny w ramach projektu „Cyberbezpieczne Wodociągi" realizowanego przez Przedsiębiorstwo Wodociągów i Kanalizacji Sp.z o.o. w Wołominie, w ramach Inwestycji C3.1.1 „Cyberbezpieczeństwo – CyberPL" – Cyberbezpieczne Wodociągi, finansowanego z Krajowego Planu Odbudowy i Zwiększania Odporności"

ja (imię i nazwisko) .....

w imieniu reprezentowanej przeze mnie firmy.....

.....

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 7 ust. 1 ww. Ustawy [1]
2. Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. 7 ust. 1 pkt ..... ww. Ustawy (podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 7 ust. 1 pkt 1, 2, 3 Ustawy).

Miejsce i data..... Podpis.....

Podpis osoby lub osób figurujących w rejestrach lub wpisie do ewidencji lub we właściwym pełnomocnictwie uprawnionych do zaciągania zobowiązań

[1] Niepotrzebne skreślić

Cyberbezpieczne Wodociągi

OŚWIADCZENIE WYKONAWCY

WYKLUCZENIE Z POSTĘPOWANIA NA PODSTAWIE ART. 5k ROZPORZĄDZENIA 833/2014 W BRZMIENIU NADANYM ROZPORZĄDZENIEM (UE) 2022/576 W SPRAWIE ZMIANY ROZPORZĄDZENIA (UE) NR 833/2014 DOTYCZĄCEGO ŚRODKÓW OGRANICZAJĄCYCH W ZWIĄZKU Z DZIAŁANIAMI ROSJI DESTABILIZUJĄCYMI SYTUACJĘ NA UKRAINIE (DZ. URZ. UE NR L 111 Z 8.04.2022)

Przystępując do postępowania o udzielenie zamówienia na:

„Opracowanie dokumentacji i wykonanie audytów – obszar organizacyjny w ramach projektu „Cyberbezpieczne Wodociągi" realizowanego przez Przedsiębiorstwo Wodociągów i Kanalizacji Sp.z o.o. w Wołominie, w ramach Inwestycji C3.1.1 „Cyberbezpieczeństwo – CyberPL" – Cyberbezpieczne Wodociągi, finansowanego z Krajowego Planu Odbudowy i Zwiększania Odporności"

ja (imię i nazwisko) .....

w imieniu reprezentowanej przeze mnie firmy.....

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 5k w/w Rozporządzenia[2]
2. Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. 5k pkt ..... Ustawy (podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 5k pkt 1, 2, 3 w/w Rozporządzenia).

Miejsce i data..... Podpis.....

Podpis osoby lub osób figurujących w rejestrach lub wpisie do ewidencji lub we właściwym pełnomocnictwie uprawnionych do zaciągania zobowiązań

Oświadczam, że 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.

Miejsce i data..... Podpis.....

Podpis osoby lub osób figurujących w rejestrach lub wpisie do ewidencji lub we właściwym pełnomocnictwie uprawnionych do zaciągania zobowiązań

[2] Niepotrzebne skreślić

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU