UMOWA
na wykonanie usługi Audytu Bezpieczeństwa

ZWIK/DO/…./2021

zawarta w Grodzisku Mazowiecki, **dnia .....** pomiędzy:

Zakładem Wodociągów i Kanalizacji Spółką z ograniczoną odpowiedzialnością z siedzibą w Grodzisku Mazowieckim (05-825) przy ul. Cegielnianej 4, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XIV Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000321963, wysokość kapitału zakładowego 29.771 000,00 PLN (w całości pokrytego), posiadającą NIP: 529-17-62-897 oraz Regon: 141717237 (zwaną dalej „Zamawiającym"), reprezentowaną przez:
reprezentowaną przez:

……..

……..
zwana dalej **Zamawiającym,**

a:

……
……
zwana dalej **Wykonawcą**

§ 1
Definicje

1. Umowa – niniejsza umowa.
2. Dzień Roboczy – każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
3. Audyt Bezpieczeństwa – czynności polegające na usiłowaniu przełamania lub ominięcia stosowanych przez Zamawiającego zabezpieczeń systemu Informatycznego przed nieuprawnionym dostępem, w celu wykrycia uchybień i luk w stosowanych przez Zamawiającego zabezpieczeniach.
4. Raport – dokument zawierający wyniki Audytu Bezpieczeństwa zawierający opis stanu Systemu Informatycznego Zamawiającego, wszystkie stwierdzone w wyniku Audytu Bezpieczeństwa uchybienia i luki w stosowanych przez Zamawiającego zabezpieczeniach Systemu Informatycznego, a także zalecenia co do działań mających na celu usunięcie stwierdzonych uchybień i luk (szczegółowa zawartość Raportu została określona w Załączniku nr 4).
5. System Informatyczny – system podlegający Audytowi Bezpieczeństwa umieszczony w Środowisku Produkcyjnym.
6. Środowisko Produkcyjne – wydzielona część środowiska informatycznego Zamawiającego służąca do gromadzenia i przetwarzania rzeczywistych danych biznesowych Zamawiającego.
7. Harmonogram prac – szczegółowy terminarz realizacji przedmiotu Umowy.
8. Rekontrola – sprawdzenie przez Wykonawcę czy wskazane w Raporcie z testów podatności zostały prawidłowo wyeliminowane przez Zamawiającego.

§ 2
Przedmiot Umowy

1. Zamawiający zamawia, a Wykonawca zobowiązuje się do:
   a) wykonania harmonogramu realizacji Audytu Bezpieczeństwa Systemu Informatycznego Zamawiającego. **Harmonogram powinien być przedstawiony Zamawiającemu w terminie do 7 dni od dnia zawarcia umowy.** Harmonogram podlega akceptacji przez Zamawiającego. Wykonawca przystąpi do realizacji Audytu Bezpieczeństwa Systemu Informatycznego Zamawiającego dopiero po akceptacji harmonogramu wykonania testów
   b) wykonania usługi Audytu Bezpieczeństwa Systemu Informatycznego Zamawiającego zgodnie z założeniami opisanymi w **Załączniku nr 8.**
   c) przekazania Zamawiającemu Raportów z testów,
   d) Wykonania Rekontroli zakończonej przesłaniem Raportu po Rekontroli.

§3
Termin realizacji Przedmiotu Umowy

1. Wykonawca przystąpi do wykonywania Przedmiotu Umowy niezwłocznie po zawarciu Umowy.
   Wykonawca jest zobowiązany do wykonania Przedmiotu Umowy w terminie 7 tygodni od dnia zgłoszenia gotowości Systemu do testów przez ZamawiającegoTermin gotowości Zamawiającego do rekontroli (maksymalna liczba dni między przekazaniem raportu z testów do Zamawiającego, a gotowością Zamawiającego do rekontroli) wynosi 15 dni roboczych.

§ 4
Obowiązki Wykonawcy

1. Wykonawca zobowiązuje się wykonać przedmiot Umowy w terminie określonym w Harmonogramie, przy dołożeniu należytej staranności.
2. Wykonawca przedstawi zespół co najmniej dwóch osób oddelegowanych do realizacji przedmiotu umowy.
3. Wykonawca zobowiązuje się do wykonania i dostarczenia Zamawiającemu Raportu w terminie określonym w Harmonogramie prac.
4. Wykonawca zobowiązuje się do informowania na bieżąco o sytuacjach niezależnych od niego, które mogą mieć wpływ na jakość i termin wykonania przedmiotu Umowy.
5. Wykonawca zastrzega sobie możliwość przeprowadzenia w ramach Audytu Bezpieczeństwa dodatkowych testów, niewymienionych w Załączniku nr 8.

§ 5
Obowiązki Zamawiającego

1. Zamawiający udostępni Wykonawcy wszelkie informacje niezbędne do wykonania Umowy.
2. Zamawiający zobowiązany jest do zapewnienia Wykonawcy, dostępu do Systemu Informatycznego, przez cały okres trwania audytu Bezpieczeństwa.

§ 6
Odbiór

1. Odbiór Raportu z testów zostanie dokonany przez przedstawicieli Zamawiającego, w terminie do 5 dni roboczych od daty dostarczenia przez Wykonawcę Raportu.
2. Odbiór Raportu z testów nastąpi w formie protokołu odbioru podpisanego i dostarczonego Wykonawcy w terminie określonym w ust 1 powyżej. Wzór protokołu odbioru określony został w **Załączniku nr 5.** W przypadku zastrzeżeń Zamawiającego co do zakresu wykonanego Audytu Bezpieczeństwa Zamawiający, w terminie określonym w ust 1 powyżej, zobowiązany jest do sporządzenia i dostarczenia Wykonawcy protokołu rozbieżności, którego wzór określony został w **Załączniku nr 6.**
3. W przypadku podpisania Protokołu Rozbieżności przez Wykonawcę, Wykonawca przystąpi do usunięcia wyszczególnionych w protokole zastrzeżeń. Po wykonaniu ww. czynności zostanie powtórzona procedura przewidziana w niniejszym paragrafie z zastrzeżeniem, że nowe zastrzeżenia mogą dotyczyć wyłącznie zastrzeżeń wymienionych w poprzednich Protokołach Rozbieżności.
4. Protokół podpisany na zasadach określonych w ust 2 z zastrzeżeniem ustępu 3 powyżej stanowi potwierdzenie prawidłowego wykonania przez Wykonawcę przedmiotu Umowy w zakresie wskazanym w § 2 ust. 1 pkt a) i b) i stanowi podstawę zapłaty wynagrodzenia określonego w § 6 ust. 1 pkt a) Umowy.
5. Odbiór Raportu po Rekontroli zostanie dokonany przez przedstawicieli Zamawiającego **w terminie do 5 dni roboczych od daty dostarczenia przez Wykonawcę Raportu**. Do odbioru Raportu po Rekontroli stosuje się odpowiednio postanowienia ust. 2 i 3 niniejszego paragrafu. Protokół z odbioru Raportu po Rekontroli stanowi potwierdzenie prawidłowego wykonania przez Wykonawcę przedmiotu Umowy w zakresie wskazanym w § 2 ust. 1 pkt c) i stanowi podstawę zapłaty wynagrodzenia określonego w § 6 ust. 1 pkt b) Umowy.
6. Osobą upoważnioną do koordynowania, uzgadniania i kontrolowania realizacji prac objętych Umową oraz podpisania protokołu odbioru ze strony Zamawiającego jest:

   ……
7. Osobą upoważnioną do koordynowania, uzgadniania i kontrolowania realizacji prac objętych Umową oraz podpisania protokołu odbioru ze strony Wykonawcy jest:

   ……

§ 7
Wynagrodzenie

1. Wynagrodzenie za wykonanie Audytu Bezpieczeństwa Systemu Informatycznego wynosi:

   a) Audyt Bezpieczeństwa Systemu Informatycznego: **……..… PLN netto,.**

   b) Rekontrola: **…….. PLN netto**
2. Do podanej w ustępie 1 powyżej kwoty netto zostanie doliczony podatek VAT w wysokości obowiązującej w dniu wystawienia faktury.
3. Wynagrodzenie, o którym mowa w ustępie 1 powyżej płatne będzie na postawie faktur wystawionych przez Wykonawcę na podstawie protokołów odbioru, o których mowa w § 5 ustęp 4 i 5.
4. Zapłata wynagrodzenia, o którym mowa w niniejszej Umowie nastąpi w terminie 30 dni od daty wystawienia faktury VAT, przelewem na rachunek bankowy Wykonawcy nr …….

5. Wykonawca jest uprawniony do przesyłania Zamawiającemu ustrukturyzowanych faktur elektronicznych za pośrednictwem platformy, zgodnie z przepisami ustawy z dnia 9.11.2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym (Dz.U. z 2018 r. poz. 2191).
6. Zamawiający może dokonywać płatności wynagrodzenia z wykorzystaniem mechanizmu podzielonej płatności.

§ 8
Odpowiedzialność

1. W przypadku zaistnienia opóźnienia niezawinionego przez Wykonawcę, a w szczególności wynikającego z niewykonania przez Zamawiającego obowiązków, o których mowa w § 4, Harmonogram prac ulega zmianie w taki sposób, że dotychczasowe terminy ulegają przesunięciu o liczbę dni opóźnienia..
2. W wypadku opóźnienia w zapłacie wynagrodzenia należnego Wykonawcy Zamawiający zapłaci Wykonawcy odsetki ustawowe od należnej kwoty za każdy dzień opóźnienia.
3. Całkowita odpowiedzialność Wykonawcy z wszelkich tytułów wynikających z Umowy oraz obowiązujących przepisów prawa nie przekroczy 100% wartości wynagrodzenia określonego w § 6 ust. 1. Ograniczenie odpowiedzialności nie obejmuje szkód wyrządzonych przez Wykonawcę z winy umyślnej.
4. Zamawiający oświadcza, iż posiada wszelkie prawa do Systemu Informatycznego, a przeprowadzenie przez Wykonawcę Audytu Bezpieczeństwa nie będzie naruszało praw osób trzecich do Systemu Informatycznego.

§ 9
Poufność

1. Dla celów niniejszej umowy przyjmuje się, że Informacje Poufne to informacje dotyczące systemu informatycznego Zamawiającego, które:
   a) zostały ujawnione Wykonawcy przez Zamawiającego w formie pisemnej lub drogą elektroniczną po dniu zawarcia niniejszej umowy i
   b) zostały wyraźnie oznaczone jako poufne i
   c) zostały zabezpieczone przez Zamawiającego w sposób uniemożliwiający uzyskanie do nich dostępu przez osoby trzecie.
2. Wykonawca zobowiązuje się do zachowania w poufności wszelkich Informacji Poufnych oraz do nieujawniania Informacji Poufnych osobom trzecim, z wyjątkiem tych osób, którym ujawnienie Informacji Poufnych jest niezbędne do realizacji prac objętych Umową.
3. Zobowiązanie, o którym mowa w ust 2 nie dotyczy informacji:
   a) na których przekazanie, ujawnienie i wykorzystanie druga Strona wyraziła uprzednią zgodę w formie pisemnej, lub
   b) są powszechnie znane
   c) danych finansowych Umowy – na potrzeby obsługi księgowej
   d) o fakcie zawarcia Umowy oraz o jej przedmiocie
   e) które Wykonawca w sposób zgodny z prawem uzyskał od osób trzecich
   f) które muszą być ujawnione organom rządowym, administracyjnym, samorządowym lub sądowym na ich żądanie zgodnie z obowiązującymi przepisami prawa
   g) które zostały przekazane w formie umożliwiającej odczyt przez osoby trzecie lub nie zostały oznaczone jako poufne.
4. Obowiązek zachowania w poufności informacji, o których mowa w niniejszym paragrafie wiąże Strony przez 2 lata od chwili zawarcia niniejszej Umowy.

§10

Siła wyższa

1. Żadna ze Stron nie ponosi odpowiedzialności za niewykonanie lub nienależyte wykonanie zobowiązań wynikających z Umowy, jeżeli jest ono następstwem siły wyższej rozumianej jako zdarzenie obiektywne, zewnętrzne, nie posiadające swojego źródła wewnątrz przedsiębiorstwa, niemożliwe do przewidzenia, nieoczekiwane, którego skutków nie da się przewidzieć i nie można im zapobiec, które wystąpiło mimo dołożenia należytej staranności wymaganej w stosunkach kupieckich (art.355 §2 kodeksu cywilnego) w celu należytego spełnienia świadczenia.
2. Strona powołująca się na zaistnienie przeszkody, o której mowa w ust 1 zobowiązana jest niezwłocznie po jej zaistnieniu oraz po powzięciu wiadomości o wpływie przeszkody na swoją zdolność do wykonania zobowiązań wynikających z Umowy, zawiadomić drugą Stronę o zaistnieniu przeszkody i jej wpływie na swoją zdolność do wykonania zobowiązań wynikających z Umowy. Do dokonania zawiadomienia Strona zobowiązana jest również w razie ustąpienia przeszkody, o której mowa w ust 1.
3. Przyczyna zwolnienia wymieniona w ust 1 jest skuteczna od momentu zaistnienia wydarzenia. Strona, która nie zawiadomi o wydarzeniu jest odpowiedzialna za szkody poniesione przez drugą Stronę, których można było uniknąć w przypadku terminowego zawiadomienia.
4. Przyczyna zwolnienia od odpowiedzialności wymieniona w ust 1 zwalnia Stronę nie wywiązującą się, z obowiązku zapłaty odszkodowania, kar umownych oraz innych odszkodowań tak długo, jak utrzymują się przyczyny wyłączenia odpowiedzialności oraz w proporcji do stopnia, w jakim istnienie tych przyczyn realnie uniemożliwia realizację zobowiązań Strony w pełnym zakresie przewidzianym Umową.
5. Przyczyna zwolnienia od odpowiedzialności wymienionej w ust 1 przedłuża termin realizacji Umowy o okres, przez jaki wykonywanie przedmiotu Umowy było niemożliwe ze względu na działanie siły wyższej, tym samym wyłączając ewentualne prawo drugiej Strony do wypowiedzenia lub odstąpienia od Umowy. Przy określaniu uzasadnionego okresu należy wziąć pod uwagę zdolność Strony nie wykonującej świadczenia do ponownego rozpoczęcia realizacji Umowy oraz zainteresowanie drugiej Strony otrzymaniem świadczenia pomimo opóźnienia. W czasie oczekiwania na kontynuację wykonania przez Stronę, która je przerwała, druga Strona może zawiesić wykonanie swoich zobowiązań.

§ 11

Prawa autorskie

Z dniem odbioru przez Zamawiającego Raportów i innych dzieł autorskich wykonanych w ramach Przedmiotu Umowy oraz innych dzieł w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2019 r. poz. 1231) Wykonawca przenosi na Zamawiającego, w ramach wynagrodzenia umownego, całość majątkowych praw autorskich do tych dzieł i ich egzemplarzy, na wszystkich znanych polach eksploatacji.

§ 12

Kary umowne

1. Wykonawca zapłaci Zamawiającemu kary umowne w następujących przypadkach:
   a) w razie zwłoki z wykonaniem przedmiotu umowy w zakresie Raportu z testów – w wysokości 2% wynagrodzenia brutto określonego w § 6 ust. 1 pkt a) Umowy za każdy dzień zwłoki,
   b) w razie zwłoki z wykonaniem przedmiotu umowy w zakresie Raportu po Rekontroli – w wysokości 2% wynagrodzenia brutto określonego w § 6 ust. 1 pkt b) Umowy za każdy dzień zwłoki,

c) w razie odstąpienia od umowy przez którąkolwiek ze Stron z przyczyn leżących po stronie Wykonawcy - 30 % sumy wynagrodzeń brutto określonych w § 6 ust. 1 pkt a) i b) Umowy.

2. Zamawiający może potrącać kary umowne z wynagrodzenia należnego Wykonawcy.
3. Suma kar umownych nie może przekroczyć 30% sumy wynagrodzeń brutto określonych w § 6 ust. 1 pkt a) i b) Umowy.
4. W przypadku gdy szkoda Zamawiającego przeniesie sumę kar umownych Zamawiający jest uprawniony do dochodzenia odszkodowania ponad wysokość kar umownych na zasadach ogólnych.

§ 13

1. Administratorem danych osobowych pozyskanych od Wykonawcy w ramach wykonywania niniejszej Umowy jest Zamawiający.
2. Wykonawca oświadcza, że znany jest mu fakt, iż treść niniejszej Umowy, a w szczególności dotyczące go dane identyfikujące, przedmiot umowy i wysokość wynagrodzenia, stanowią informację publiczną w rozumieniu art. 1 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (j.t. Dz. U. z 2016 r. poz. 1764), która podlega udostępnianiu w trybie przedmiotowej ustawy.
3. W ramach wykonania obowiązku informacyjnego, zgodnie z rozporządzeniem Parlamentu Europejskiego i rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich informacji danych (Dz. Urz. UE L 119 z 04.05.2016) - dalej RODO, oraz uchylenia dyrektywy 95/46/WE, Wykonawca poinformuje osoby, których jakiekolwiek dane osobowe zostały przekazane Zamawiającemu, o posiadaniu i przetwarzaniu danych osobowych tych osób przez Zamawiającego w celu wykonywania niniejszej Umowy. Wykonawca zobowiązany jest także poinformować osoby, o których mowa w zdaniu poprzednim, o prawie dostępu do treści danych, ich poprawiania, modyfikacji oraz możliwości skorzystania z innych uprawnień przewidzianych unormowaniami RODO.
4. Informacja o przetwarzaniu danych osobowych stanowi Załącznik do niniejszej Umowy.

§ 14

Postanowienia końcowe

1. Na podstawie art. 4c ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych Zamawiający oświadcza, że posiada status dużego przedsiębiorcy w rozumieniu art. 3 ust. 4 załącznika I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i art. 108 Traktatu (Dz.Urz. UE L 187 z 26.06.2014, str. 1, z późn. zm.).
2. Wszelkie spory wynikające z Umowy rozstrzygane będą przez sąd powszechny właściwy miejscowo dla siedziby Wykonawcy.
3. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
4. W sprawach nieuregulowanych niniejszą Umową mają zastosowanie przepisy kodeksu cywilnego, ustawy o prawie autorskim i prawach pokrewnych oraz inne obowiązujące przepisy prawa.
5. Umowa została sporządzona w dwóch jednobrzmiący egzemplarzach, po jednym dla każdej ze Stron.
6. Integralną cześć Umowy stanowią następujące załączniki:

a) Załącznik nr 1 – KRS Zamawiającego
b) Załącznik nr 2 – KRS/CEIDG Wykonawcy
c) Załącznik nr 3 - Harmonogram prac
d) Załącznik nr 4 - Zakres Raportów
e) Załącznik nr 5 – Wzór protokołu odbioru
f) Załącznik nr 6 – Wzór protokołu rozbieżności

g) Załącznik nr 7 - Informacja o przetwarzaniu danych osobowych
h) Załącznik nr 8 – Specyfikacja przedmiotu umowy
i) Załącznik nr 9 – Wykaz osób oddelegowanych przez Wykonawcę do realizacji umowy.
j) Załącznik nr 10 - Umowa powierzenia przetwarzania danych osobowych

_____	_____
Zamawiający	Wykonawca

Załącznik nr 3 - Harmonogram prac

Termin wykonania Audytu Bezpieczeństwa: do ……. od dnia rozpoczęcia prac.

Termin rozpoczęcia prac zostanie ustalony przez Strony w trybie roboczym.

Termin dostarczenia Raportu: do ……od dnia zakończenia Audytu Bezpieczeństwa

Termin wykonania Rekontroli: do ……od dnia zgłoszenia przez Zamawiającego gotowości do wykonania Rekontroli

Terminy opisane powyżej zostaną zachowane pod warunkiem spełnienia przez Zamawiającego obowiązków wynikających z Umowy, w szczególności zapewnienia stosownych dostępów do audytowanych systemów.

W wyniku prac dostarczone zostaną dwa typy raportów, których charakterystyka została przedstawiona poniżej.

Szablon raportu testów

Raport końcowy podsumowujący całość testów penetracyjnych powinien zawierać następujące informacje:

- Zakres przeprowadzonych prac
- Przebieg realizacji prac (harmonogram)
- Opis metodyki przeprowadzonych testów
- Definicja przyjętej klasyfikacji zagrożenia w przypadku wykorzystania podatności
- Opis każdej z luk zawierać powinien następujące elementy:
    - Nazwa podatności
    - Opis podatności – szczegółowy opis zasady działania podatności
    - Przykładowy wektor ataku: scenariusz wykorzystania podatności do wykonania ataku
    - Poziom zagrożenia wg. przyjętej definicji
    - Narzędzia użyte do wykrycia i wykorzystania podatności (nazwa, wersja)
    - Typ podatności – ogólna charakterystyka kategoria podatności
    - Zalecenia dotyczące wyeliminowania podatności
    - Odniesienie do punktu z OWASP WSTG - v4.1 Table of Contents

Edytowalna wersja zestawienia wykrytych podatności w arkuszu kalkulacyjnym

Wykryte podatności powinny zostać opisane w edytowalnej wersji arkusza kalkulacyjnego (preferowany Excel) wg. poniższego wzorca.

(1) Identyfikacja podatności						
Nazwa hosta	**Adres IP**	**Nazwa podatności**	**Opis podatności**	**Poziom ryzyka**	**Rekomendacje**	**Odniesienie do punktu z OWASP WSTG - v4.1 Table of Contents**

Załącznik nr 5 – Wzór protokołu odbioru

……, dnia ……..

Protokół odbioru

Zamawiający**:** …….

Reprezentowany przez ……

potwierdza prawidłową realizację następującego zakresu prac:

…….

Prace zgodne z umową: …….

Wykonawca:

Przedstawiciel Zamawiającego	Przedstawiciel Wykonawcy
……	
…….	
Podpis	Podpis

Załącznik nr 6 – Wzór protokołu rozbieżności

……, dnia ……..

Protokół rozbieżności

Dotyczy Raportu z dnia: ……wykonanego na bazie Umowy nr ……z dnia…….

Zamawiający**:** …….

Reprezentowany przez: ……..

zgłasza następujące uwagi do Raportu:

…….
…….
…….

Wykonawca:

Przedstawiciel Zamawiającego	Przedstawiciel Wykonawcy
……	……
Podpis	Podpis

Załącznik nr 7 do umowy

Informacja o przetwarzaniu danych osobowych

Zamawiający - Zakład Wodociągów i Kanalizacji Sp. z o.o. w Grodzisku Mazowieckim informuje, że:

a) Dane osobowe Wykonawców, osób reprezentujących Wykonawców, pełnomocników i innych osób wskazanych w ofercie lub załączonych do niej dokumentach oraz umowie i jej załącznikach są przetwarzane przez Zakład Wodociągów i Kanalizacji Sp. z o.o., ul. Cegielniana 4, 05-825 Grodzisk Mazowiecki.

b) W Zakładzie Wodociągów i Kanalizacji Sp. z o.o. w Grodzisku Mazowieckim został powołany inspektor ochrony danych: Piotr Franaszczuk który jest dostępny pod nr tel. 22 724 30 36, adres e-mail: praca@zwik-grodzisk.pl, ul. Cegielniana 4, 05-825 Grodzisk Mazowiecki.

c) Dane osobowe są przetwarzane w celu wykonywania umowy (podstawa prawna: Art. 6 ust. 1 pkt b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz.UE.L 2016 Nr 119, str. 1).

d) Odbiorcami danych osobowych mogą być: Urząd Miasta Grodzisk Mazowiecki.

e) Zakład Wodociągów i Kanalizacji Sp. z o.o. w Grodzisku Mazowieckim nie zamierza przekazywać danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

f) Dane osobowe będą przechowywane przez okres obowiązywania umowy oraz przez minimum 6 lat po zakończeniu obowiązywania umowy w celu spełnienia obowiązków wynikających z przepisów dotyczących dokumentowania zdarzeń gospodarczych, z uwzględnieniem upływu terminu przedawnienia zobowiązań podatkowych.

g) Wykonawcy, osoby reprezentujące Wykonawców, pełnomocnicy i inne osoby wskazane w ofercie lub załączonych do niej dokumentach oraz umowie i jej załącznikach mają prawo do żądania dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.

h) Wykonawcy, osoby reprezentujące Wykonawców, pełnomocnicy i inne osoby wskazane w ofercie lub załączonych do niej dokumentach oraz umowie i jej załącznikach mają prawo do wniesienia skargi do organu nadzorczego:

   Urząd Ochrony Danych Osobowych, ul. Stawki 2; 00-193 Warszawa; tel. 22 531 03 00; fax 22 531 03 01; email: kancelaria@uodo.gov.pl

i) Podanie danych osobowych jest warunkiem zawarcia umowy. Niepodanie danych będzie skutkowało niemożnością realizacji umowy.

j) Dane osobowe nie podlegają profilowaniu.

Zapoznałem się

……

Data i podpis

Załącznik nr 8

Przedmiot zapytania

Przedmiotem zapytania jest

1.) Przeprowadzenie testów penetracyjnych dla portalu dostępnego w Internecie pod adresem https://ebok.zwik-grodzisk.pl
2.) Przedstawienie raportów opracowanych w oparciu o przeprowadzone testy penetracyjne, które powinny obejmować co najmniej:
    a. Podsumowanie dla kierownictwa
    b. Podsumowanie zidentyfikowanych podatności i rekomendacji
    c. Opis zastosowanych metodyk i technik.
    d. Opis założeń przyjętych do testowania oraz ewentualnych wykluczeń
    e. Zestawienie informacji o przeprowadzonych testach, w tym informacje o testowanych adresach IP, przeprowadzonych testach
    f. Zrzuty ekranów i/lub listing poleceń źródłowych stanowiące dowód występowania podatności (tam gdzie ma to zastosowanie)
    g. Zestawienie zidentyfikowanych podatności w postaci tabeli zawierającej, co najmniej: identyfikator podatności, nazwę , opis, opis wpływu, prawdopodobieństwo jej wykorzystania oraz sposoby jej wyeliminowania.
    h. Zestawienie rekomendacji dotyczących minimalizacji zidentyfikowanych ryzyk.
    i. Informacje o osobach realizujących badania.
    j. Pozyskane informacje o testowanych systemach.
3.) Przeprowadzenie warsztatów, podczas których zostaną przedstawione i omówione wyniki badań.

Wymagania

Sposób realizacji testów

REQ 1. Testy muszą zostać przeprowadzone w oparciu o zasadę *grey box testing*.

REQ 2. Testy muszą założyć dwa scenariusze postępowania:
a. Testy aplikacji bez posiadania danych do logowania do aplikacji.
b. Testy aplikacji z poziomu uwierzytelnionego użytkownika.

Testy prowadzone mają być bez dostępu do kodów źródłowych aplikacji oraz informacji o technologii wykonani

REQ 3. Testy penetracyjne muszą objąć także badania dotyczące zweryfikowania, czy korzystając z konta użytkownika możliwa jest eskalacja dostępów na poziomie systemów operacyjnych, baz danych i innych komponentach powiązanych z aplikacją.

REQ 4. Zakres testów musi być oparty o wytyczne zawarte w dokumencie OWASP Web Security Testing Guide v4.1
Jeżeli wykonanie któregoś z rodzajów z testów nie będzie możliwe lub nie będzie miało zastosowania wówczas taka informacja powinna zostać umieszczona w raporcie

REQ 5. Testy nie mogą być realizowane tylko z wykorzystaniem narzędzi automatycznych, konieczna jest manualna weryfikacja podatności znalezionych w testach automatycznych. Dodatkowo należy manualnie zweryfikować wszystkie krytyczne funkcjonalności w testowanej aplikacji webowej.

REQ 6. Ocena wpływu wykrytej podatności musi zostać podana w sposób opisowy w postaci wyszczególnienia potencjalnych konsekwencji.

REQ 7. Przeprowadzenie testów nie może wymagać od Zamawiającego zakupu żadnych dodatkowych licencji lub wyposażenia.

Bezpieczeństwo realizacji

REQ 8. Testy zostaną przeprowadzone na środowisku produkcyjnym.

REQ 9. Testy nie mogą naruszyć prawidłowego działania tego środowiska. Ustalone muszą zostać terminy wykonywania testów.
Może zajść konieczność wykonania testów poza standardowymi godzinami pracy (8-15).

REQ 10. W trakcie badań nie zostaną wyłączone żadne istniejące i działające zabezpieczenia.

REQ 11. Testy muszą zostać przeprowadzone zgodnie zasadami oraz harmonogramem ustalonym z Zamawiającym.

Zespół realizacyjny

REQ 12. Oferent musi przedstawić skład personalny zespołu wdrożeniowego wraz z opisem doświadczenia zawodowego każdego z członków zespołu.

REQ 13. Oferent musi dysponować odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia a w tym:

Wykazać dysponowanie minimum dwiema osobami, posiadającymi przynajmniej 3 - letnie doświadczenie w zakresie testowania bezpieczeństwa systemów informatycznych
Przynajmniej jedna z tych osób musi posiadać jeden z certyfikatów: OSCP (Offensive Security Certified Professional) lub CEH (Certified Ethical Hacker) oraz
Przynajmniej jedna z tych osób musi posiadać jeden z certyfikatów: : CISA (aktualnym i wydanym przez isaca.org) lub CISSP (aktualnym i wydanym przez ISC2.org) lub Lead Auditor ISO27001 (aktualnym i wydanym przez akredytowane organizacje certyfikujące)

REQ 14. Oferent powinien zapewnić niezmienność zespołu projektowego w trakcie realizacji projektu.

REQ 15. Każda zmiana składu zespołu projektowego musi być zaakceptowana przez Zamawiającego.

Szablon raportu testów penetracyjnych

Raport końcowy podsumowujący całość testów penetracyjnych powinien zawierać następujące informacje:

- Zakres przeprowadzonych prac
- Przebieg realizacji prac (harmonogram)
- Opis metodyki przeprowadzonych testów
- Definicja przyjętej klasyfikacji zagrożenia w przypadku wykorzystania podatności
- Opis każdej z luk zawierać powinien następujące elementy:
  - Nazwa podatności
  - Opis podatności – szczegółowy opis zasady działania podatności
  - Przykładowy wektor ataku: scenariusz wykorzystania podatności do wykonania ataku
  - Poziom zagrożenia wg. przyjętej definicji
  - Narzędzia użyte do wykrycia i wykorzystania podatności (nazwa, wersja)
  - Typ podatności – ogólna charakterystyka kategoria podatności
  - Zalecenia dotyczące wyeliminowania podatności
  - Odniesienie do punktu z OWASP WSTG - v4.1 Table of Contents

Edytowalna wersja zestawienia wykrytych podatności w arkuszu kalkulacyjnym

Wykryte podatności powinny zostać opisane w edytowalnej wersji arkusza kalkulacyjnego (preferowany Excel) wg. poniższego wzorca.

(1) Identyfikacja podatności						
Nazwa hosta	**Adres IP**	**Nazwa podatności**	**Opis podatności**	**Poziom ryzyka**	**Rekomendacje**	**Odniesienie do punktu z OWASP WSTG - v4.1 Table of Contents**

Załącznik nr 9

Wykaz osób

Na podstawie umowy nr ZWIK/DO/…./2021 zawartej w dniu ……..……..…… r.

1. Przedmiot Umowy zostanie wykonany poprzez oddelegowany zespół dwóch osób:

Lp.	Imię i nazwisko	Posiadane certyfikaty	Opis posiadanego doświadczenia z przeprowadzenia audytu lub testów bezpieczeństwa informatycznego systemów informatycznych	Nazwa podmiotu, na rzecz którego był przeprowadzany audyt lub test bezpieczeństwa wraz z podaniem dat od-do
1.				
2.				

……..

Podpis Wykonawcy

Załącznik nr 10
do umowy na wykonanie usługi Audytu Bezpieczeństwa

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu ……. w Grodzisku Mazowieckim pomiędzy:

Zakładem Wodociągów i Kanalizacji Sp. z o.o. z siedzibą w Grodzisku Mazowieckim (05-825), przy ul. Cegielnianej 4, wpisaną do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XIV Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000321963, wysokość kapitału zakładowego 29 771 000,00 zł, posiadającą NIP: 529-17-62-897 oraz Regon: 141717237, reprezentowaną przez:

1. **…….**
2. **……..**

zwanym dalej **Administratorem**

a

……

zwaną dalej **Podmiotem przetwarzającym**

zwanymi każdą z osobna w dalszej części Umowy „**Stroną**”, a łącznie „**Stronami**”.

Zważywszy, że na podstawie umowy z dnia …….. nr …… o wykonanie usługi Audytu bezpieczeństwa systemu informatycznego: https://ebok.zwik-grodzisk.pl (zwanej dalej „Umową Główną”) :

- Podmiot przetwarzający będzie wykonywał audyt bezpieczeństwa na rzecz Administratora, ,
- Podmiot przetwarzający w ramach usług, będzie miał dostęp do danych osobowych Baza klientów ZWIK w zakresie: imienia, nazwiska , nr telefonu, adres email, adres klienta, nr klienta, zużycia wody przetwarzanych u Administratora ,

Strony niniejszym, postanawiają zawrzeć Umowę powierzenia przetwarzania danych osobowych („Umowa”), o następującej treści:

§ 1
Oświadczenia Stron

1. Przetwarzanie danych osobowych w związku z wykonywaniem Umowy Głównej odbywać się będzie w zgodzie i w oparciu o Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) zwanego dalej „RODO“.
2. Administrator w trybie art. 28 ust. 3 RODO powierza Podmiotowi przetwarzającemu do przetwarzania dane osobowe, które zgromadził zgodnie z obowiązującymi przepisami prawa, a Podmiot przetwarzający zobowiązuje się do ich przetwarzania zgodnie z Umową.

3. Podmiot przetwarzający oświadcza, że dysponuje zasobami, doświadczeniem, wiedzą fachową i wykwalifikowanym personelem, które umożliwiają mu prawidłowe wykonanie Umowy Powierzenia oraz wdrożenie odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO.
4. Podmiot przetwarzający oświadcza również, że osobom zatrudnionym przy przetwarzaniu powierzonych danych osobowych nadane zostały upoważnienia do przetwarzania danych osobowych, o których mowa w art. 29 RODO oraz że osoby te zostały zapoznane z przepisami o ochronie danych osobowych oraz z odpowiedzialnością za ich nieprzestrzeganie, zobowiązały się do ich przestrzegania oraz do bezterminowego zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczenia.

§ 2

Cel, zakres, miejsce przetwarzania powierzonych danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych Administratora, jedynie w celu wykonania audytu bezpieczeństwa systemu informatycznego: https://ebok.zwik-grodzisk.pl**.**
2. Podmiot przetwarzający zobowiązuje się do przetwarzania powierzonych danych osobowych wyłącznie w celach związanych z realizacją Umowy i wyłącznie w zakresie, jaki jest niezbędny do realizacji tych celów.
3. Zakres powierzanych danych obejmuje: dane przetwarzane w ramach usług audytu bezpieczeństwa zgodnie z Umową Główną .
4. Podmiot przetwarzający otrzymuje dostęp do następujących danych osobowych zawartych w bazach danych: **Baza klientów ZWIK w Grodzisku Mazowieckim.**
Podmiot przetwarzający zobowiązuje się do przetwarzania danych osobowych w sposób stały. Podmiot przetwarzający będzie w szczególności wykonywał następujące operacje dotyczące powierzonych danych osobowych: utrwalanie, porządkowanie, przechowywanie, wykorzystywanie (do celów wskazanych w pkt 2 powyżej), ujawnianie innym podmiotom zgodnie z przepisami prawa, postanowieniami Umowy lub na polecenie Administratora, usuwanie. Dane osobowe będą przez Podmiot przetwarzający przetwarzane w formie elektronicznej w systemach .
5. Na wniosek Administratora lub osoby, której dane dotyczą Podmiot przetwarzający wskaże miejsca, w których przetwarza powierzone dane.

§ 3

Zasady przetwarzania danych osobowych

1. Strony zobowiązują się wykonywać zobowiązania wynikające z niniejszej Umowy z najwyższą starannością zawodową w celu zabezpieczenia prawnego, organizacyjnego i technicznego interesów Stron w zakresie przetwarzania powierzonych danych osobowych.
2. Podmiot przetwarzający zobowiązuje się zastosować środki techniczne i organizacyjne mające na celu należyte, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, zabezpieczenie powierzonych do przetwarzania danych osobowych, w szczególności zabezpieczyć je przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Podmiot przetwarzający oświadcza, że zastosowane do przetwarzania powierzonych danych systemy informatyczne spełniają wymogi aktualnie obowiązujących przepisów prawa.
4. Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora.
5. Podmiot przetwarzający, biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw.

6. Podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO.
7. Podmiot przetwarzający zobowiązuje się przekazywać Administratorowi, w ciągu 24 godzin od wykrycia zdarzenia, informacje o naruszeniu ochrony powierzonych Podmiotowi przetwarzającemu danych osobowych, w tym informacje niezbędne Administratorowi do zgłoszenia naruszenia ochrony danych organowi nadzorczemu, o których mowa w art. 33 ust. 3 RODO.
8. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że szczególne przepisy prawa nakazują przechowywanie danych osobowych.
9. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, w tym także po rozwiązaniu niniejszej Umowy , oraz zobowiązuje się zapewnić, aby jego pracownicy oraz inne osoby upoważnione do przetwarzania powierzonych danych osobowych, zobowiązały się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, w tym także po rozwiązaniu Umowy Powierzenia.
10. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszej Umowie oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.
11. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego, bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora.
12. Podmiot przetwarzający zobowiązuje się powiadamiać Administratora niezwłocznie o:
    a) wszczęciu kontroli przez Prezesa Urzędu Ochrony Danych Osobowych lub przez inny organ nadzorczy zajmujący się ochroną danych osobowych w związku z powierzeniem Podmiotowi przetwarzającemu przetwarzania danych osobowych, a także o wszelkich decyzjach lub postanowieniach administracyjnych wydanych wobec Podmiotu przetwarzającego w związku z powyższym;
    b) wszczętych lub toczących się postępowaniach administracyjnych, sądowych lub przygotowawczych związanych z powierzeniem Podmiotowi przetwarzającemu przetwarzania danych osobowych, a także o wszelkich decyzjach, postanowieniach lub orzeczeniach wydanych wobec Podmiotu przetwarzającego w związku z powyższym;
    c) wszelkich incydentach dotyczących powierzonych do przetwarzania danych osobowych przez Administratora, w tym uzyskania przypadkowego lub nieupoważnionego dostępu do powierzonych danych osobowych, przypadkach zmiany, utraty, uszkodzenia lub zniszczenia powierzonych Podmiotowi przetwarzającemu danych osobowych.
13. Podmiot przetwarzający nie może przekazywać powierzonych mu do przetwarzania danych osobowych do podmiotów znajdujących się w państwach spoza Europejskiego Obszaru Gospodarczego.

§ 4

Odpowiedzialność Stron

1. Administrator danych ponosi odpowiedzialność za przestrzeganie przepisów prawa w zakresie przetwarzania i ochrony danych osobowych według RODO.
2. Powyższe nie wyłącza odpowiedzialności Podmiotu przetwarzającego, za przetwarzanie powierzonych danych niezgodnie z Umową.
3. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem, jeśli nie dopełnił obowiązków, które nakłada niniejsza Umowa, lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom.
4. W przypadku naruszenia przepisów o Ochronie danych osobowych z przyczyn leżących po stronie Podmiotu przetwarzającego, Podmiot ten ponosi pełną odpowiedzialność cywilną i administracyjną zgodnie z obowiązującymi przepisami prawa.

§ 5

Termin obowiązywania Umowy

1. **Niniejsza umowa zostaje zawarta na czas określony – 7 tygodni od dnia podpisania umowy (termin obowiązywania Umowy Głównej).**
2. W przypadku rozwiązania Umowy Głównej przed terminem, o którym mowa w ust. 1, niniejsza Umowa ulega rozwiązaniu z dniem rozwiązania Umowy Głównej. W przypadku przedłużenia terminu obowiązywania Umowy Głównej termin obowiązywania niniejszej Umowy przedłuża się odpowiednio do tego terminu bez konieczności składania dodatkowych oświadczeń przez którąkolwiek ze Stron.
3. Administrator może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:
    1) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
    2) przetwarza dane osobowe w sposób niezgodny z umową;
    3) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;
4. Rozwiązanie niniejszej Umowy na podstawie postanowień ust. 2 stanowi przesłankę do wypowiedzenia, rozwiązania lub odstąpienia od Umowy Głównej przez Administratora z przyczyn leżących po stronie Podmiotu przetwarzającego.

§ 6

Postanowienia końcowe

1. Wszelkie zmiany niniejszej Umowy, powinny być dokonane w formie pisemnej pod rygorem nieważności.
2. W zakresie nieuregulowanym niniejszą Umową zastosowanie mają przepisy Kodeksu cywilnego, RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000).
3. W przypadku, gdy niniejsza Umowa odwołuje się do przepisów prawa, oznacza to również inne przepisy dotyczące ochrony danych osobowych, a także wszelkie nowelizacje, jakie wejdą w życie po dniu zawarcia Umowy, jak również akty prawne, które zastąpią wskazane ustawy i rozporządzenia.
4. Wszelkie spory związane z niniejszą Umową będą rozstrzygane przez sąd powszechny właściwy dla siedziby Administratora.
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Administrator **Podmiot przetwarzający**