

Wodociągi Białostockie Sp. z o.o.

15-404 Białystok

ul. Młynowa 52/1

www.wobi.pl

Zarejestrowana w Sądzie Rejonowym w Białymstoku, XII Wydz. Gosp. Krajowego Rejestru Sądowego
Nr KRS 0000024985 NIP 542-020-01-22 Kapitał zakładowy: 165 540 000,00 zł

Centrala - tel. 85 74 58 100

Sekretariat - tel. 85 74 58 101

fax 85 74 58 113

e-mail: sekretariat@wobi.pl

Białystok, dn. 19.06.2020 r.

OGŁOSZENIE / SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA**W PRZETARGU NIEOGRANICZONYM NA**

Przeprowadzenie przeglądu cyberzagrożeń przedsiębiorstwa w oparciu o wdrożenie systemu typu GRC (Governance, Risk Management, Compliance - Ład Korporacyjny, Zarządzanie Ryzykiem, Zgodność)

Nr ref. sprawy: NI-I-3/2020

Wodociągi Białostockie Sp. z o.o. – zwana dalej „**Zamawiającym**”, na podstawie § 20 ust. 1 „Regulaminu udzielania zamówień sektorowych w sytuacji braku obowiązku stosowania przepisów ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych” – dalej zwanym „Regulaminem”, zaprasza do złożenia ofert w **przetargu nieograniczonym na „Przeprowadzenie przeglądu cyberzagrożeń przedsiębiorstwa w oparciu o wdrożenie systemu typu GRC (Governance, Risk Management, Compliance - Ład Korporacyjny, Zarządzanie Ryzykiem, Zgodność)”**

Przystąpienie do przetargu jest równoznaczne z wyrażeniem zgody przez Wykonawcę na warunki „Regulaminu udzielania zamówień sektorowych w sytuacji braku obowiązku stosowania przepisów ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych” obowiązującego w „Wodociągach Białostockich” Sp. z o.o. w Białymstoku.

Treść w/w Regulaminu jest dostępna na stronie internetowej Zamawiającego www.wobi.pl w zakładce *Przetargi; Regulaminy udzielania zamówień.*

Niniejsze ogłoszenie wraz z SIWZ zostało opublikowane na stronie internetowej bip.wobi.pl w zakładce *Przetargi* oraz wywieszono na tablicy ogłoszeń w siedzibie Zamawiającego, w Białymstoku przy ul. Młynowej 52/1.

I. OPIS PRZEDMIOTU ZAMÓWIENIA

TABELA NR 1 – opis minimalnych wymagań dla systemu do przeprowadzenia przeglądu cyberzagrożeń za pomocą jednolitej platformy do wykrywania i zarządzania incydentami, podatnościami i ryzykiem.

SYSTEM – W POSTACI JEDNEJ PLATFORMY DO WYKRYWANIA I ZARZĄDZANIA INCYDENTAMI, PODATNOŚCIAMI I RYZYKIEM – WINIEN ZAPEWNIĄĆ / POSIADAĆ:
<p>1. Narzędzia do tworzenia elektronicznej, interaktywnej dokumentacji systemu teleinformatycznego, w tym schematów architektury zabezpieczeń sieci (tzn. mapy pokazującej urządzenia zabezpieczeń, strefy bezpieczeństwa, zasoby IT, połączenia i topologię sieci), prezentującej informacje nt. bezpieczeństwa w ujęciu technicznym oraz w odniesieniu do procesów działania organizacji.</p>
<p>2. Narzędzia umożliwiające dokonanie oceny wpływu incydentu bezpieczeństwa IT na działalność organizacji, m.in. po wpisaniu adresu IP zasobu IT związanego z incydem bezpieczeństwa system winien wyszukiwać i prezentować informacje nt. procesów organizacji i klasyfikowanych informacji (m.in. danych osobowych), które mogły zostać naruszone w wyniku incydentu oraz wyświetlać przewidywane istotne dla organizacji konsekwencje naruszenia bezpieczeństwa.</p>
<p>3. Narzędzia prezentujące techniczne informacje nt. bezpieczeństwa IT z perspektywy działalności organizacji. Umożliwiać zapisywanie, wyszukiwanie i prezentowanie co najmniej następujących informacji: procesy działania organizacji, klasyfikacja zbiorów informacji, ważność zasobu IT dla organizacji, właścicieli zasobów IT oraz zespoły obsługi.</p>
<p>4. Narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa. Umożliwiać definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz umożliwiać wyszukiwanie lokalizacji zasobów IT, gdzie znajdują się dane określonej kategorii oraz wskazywać je na graficznej mapie systemu teleinformatycznego.</p>
<p>5. Narzędzia do modelowania zagrożeń (Threat Modelling) umożliwiające symulowanie różnych potencjalnych scenariuszy incydentów bezpieczeństwa IT. Winne być dostępne narzędzia działające na graficznej mapie systemu teleinformatycznego służące do m.in.:</p> <ul style="list-style-type: none">• wyznaczania źródła zagrożenia zasobu IT wraz z wynikiem analizy ryzyka dla tego zagrożenia wyliczanym w sposób automatyczny,• wyświetlania zabezpieczeń zasobu IT przed potencjalnymi źródłami zagrożenia,• wyświetlania zabezpieczeń chroniących zasoby IT przed określonym źródłem zagrożenia,• wyświetlania lokalizacji zasobów określonego rodzaju,• wyświetlania najbardziej narażonych zasobów IT,• wyświetlania ważnych zasobów IT narażonych na awarie.
<p>6. Graficzne narzędzia do definiowania wymagań bezpieczeństwa organizacji (m.in. środków ochrony wymaganych dla określonych elementów i obszarów systemu teleinformatycznego) oraz narzędzia do audytowania bezpieczeństwa (Security Audit) względem tych wymagań. Narzędzia systemu winny umożliwiać m.in.:</p> <ul style="list-style-type: none">• zweryfikowanie, czy stan bezpieczeństwa systemu teleinformatycznego odpowiada specyficznym wymaganiom organizacji,• wyznaczanie zasobów IT o wysokim poziomie ryzyka, które nie posiadają wymaganych zabezpieczeń,• wskazywanie zasobów IT o krytycznym znaczeniu dla organizacji, które nie posiadają odpowiednich zabezpieczeń
<p>7. Narzędzia graficzne do tworzenia i przeszukiwania elektronicznej dokumentacji prezentujące wyniki na schemacie mapy logicznej oraz fizycznej. Winne one umożliwiać rozbudowę elektronicznej dokumentacji o nowe parametry oraz dołączane dokumenty, odnoszące się m.in. do stref bezpieczeństwa, systemów zabezpieczeń, urządzeń fizycznych oraz zasobów informacyjno-usługowych.</p>

8. Możliwość wykrywania topologii sieci fizycznej oraz jej wizualizacji na podstawie protokołów sieciowych takich jak: SNMP v2 i v3, LLDP, CDP itp.
9. Mechanizmy umożliwiające rozpoznanie systemów IT (Asset Discovery) oraz zapisywanie wyników w module elektronicznej dokumentacji, zapewniając: <ul style="list-style-type: none"> • możliwość wykrywania zasobów oraz ich parametrów na podstawie wyników przynajmniej jednego skanera podatności, • możliwość wykrywania zasobów oraz ich parametrów na podstawie wyników przynajmniej jednego skanera sieciowego, • możliwość wykrywania zasobów oraz ich parametrów przy wykorzystaniu protokołu WMI, • możliwość wykrywania zasobów oraz ich parametrów przy wykorzystaniu skryptów SSH oraz PowerShell, • możliwość wykrywania zasobów oraz ich parametrów na podstawie interpretacji zdarzeń,
10. Bazę wiedzy eksperckiej zawierającą wiedzę pozwalającą ocenić poprawność projektu zabezpieczeń identyfikując efektywność zastosowanych mechanizmów sieciowych oraz lokalnych w stosunku do potencjalnych wektorów ataków oraz w przypadku ich nie zastosowania zidentyfikować ryzyka, które się z tym wiążą.
11. Możliwość definiowania procesów organizacji oraz zależności od innych procesów, a także zapewnić możliwość definiowania czasów ich aktywności (np. proces praca biurowa w organizacji jest aktywny od poniedziałku do piątku od 7:00 do 15:00). Zależności winne być prezentowane w postaci graficznej.
12. Możliwość definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT zdefiniowanego w elektronicznej dokumentacji oraz prezentacji tych informacji w formie graficznej.
13. Mechanizm automatyczne wyszukiwania pojedynczych punktów awarii sieci i systemów IT (Single Point of Failure) w elektronicznej dokumentacji zapisanej w systemie (tzn. elementów bez redundancji), których uszkodzenie spowoduje zablokowanie ważnych procesów organizacji.
14. Mechanizm automatycznego szacowania ryzyka dla wszystkich systemów IT zdefiniowanych w elektronicznej dokumentacji. Szacowanie ryzyka odbywać się winno względem zagrożeń natury informatycznej, np. włamanie, infekcja złośliwym programem, podsłuch sieciowy, awaria. Powiązanie systemów IT z procesami biznesowymi w celu podsumowania ryzyka wszystkich najważniejszych systemów IT.
15. Możliwość prezentacji w formie graficznej podsumowania aktualnego stanu bezpieczeństwa , m.in. procesy organizacji zagrożone przez pojedyncze punkty awarii.
16. Możliwość monitorowania aktywności stron internetowych, portów TCP, ICMP oraz mapowania czasów dostępności / niedostępności bezpośrednio na procesy biznesowe oraz procesy zależne. W przypadku gdy system wykryje niedostępność monitorowanej usługi winien generować alarm powiadamiając jednocześnie właścicieli procesów biznesowych których procesy zależą w sposób pośredni lub bezpośredni od tej usługi (np.: e-mail, SMS. Komunikator).
17. Mechanizm parsowania spływających do niego zdarzeń w następujących formatach: <ul style="list-style-type: none"> • SYSLOG; • Wiadomości e-mail; • Dziennika zdarzeń Windows (WEF – Windows Event Forwarding); Przez parsowanie zdarzeń rozumie się proces analizy zdarzenia i rozkład na elementy składowe takie jak np.: adres IP źródłowy, adres IP docelowy, data, czas, użytkownik, treść zdarzenia itp.
18. Predefiniowany zestaw parserów zdarzeń.
19. Mechanizmy umożliwiające mu pozyskanie zdarzeń z baz danych oraz plików płaskich;
20. Wbudowany interfejs graficzny do tworzenia własnych parserów umożliwiający następujące funkcjonalności: <ul style="list-style-type: none"> • Parsowanie warunkowe; • Parsowanie hierarchiczne; • Wzbogacanie zdarzeń o dodatkowe pola; • Mapowanie wartości; • Zastosowanie wyrażeń regularnych; • Wsparcie dla formatów JSON oraz XML; • Wykorzystanie gotowych parserów przy tworzeniu nowych;

<ul style="list-style-type: none"> • Mechanizmy wyszukiwania w polach zdarzeń;
21. Zbierania i przetwarzania informacji dotyczących przepływów sieciowych [ang. Netflow].
22. Analizę anomalii bazując na informacjach zbieranych z przepływów sieciowych (ang. NetFlow), gdzie w zależności od zdefiniowanych reguł będzie budował dynamiczne linie trendów wykrywając odchylenia związane z procentową zmianą poziomu transmisji.
23. Możliwość zastosowania filtrów pozwalających na analizę anomalii względem parametrów zdefiniowanych w elektronicznej dokumentacji, takich jak rodzaj zasobu, strefa bezpieczeństwa, proces biznesowy;
24. Możliwość odczytywania alarmów wysyłanych z innych systemów w tym systemów zabezpieczeń, dla których na podstawie informacji zawartych w elektronicznej dokumentacji winien automatycznie oszacować konsekwencje incydentów bezpieczeństwa (Business Impact Analysis) , m.in. jakie procesy organizacji mogą zostać zakłócone, jakie informacje klasyfikowane mogą zostać skradzione przez przestępców.
25. Mechanizmy analizy i korelacji zdarzeń z podstawowym zestawem funkcji takich jak: <ul style="list-style-type: none"> • Stale uzupełniany zestaw parserów zdarzeń dla różnych rodzajów źródeł. • Mechanizmy parsowania regex, xml, json, parsowanie warunkowe i podrzędne oraz graficzny interfejs tworzenia parserów wraz z wbudowanym debuggerem - narzędzia które są w stanie przetworzyć i znormalizować dane z dowolnego źródła. Zgromadzone dane dzięki procesowi normalizacji winne stać się informacjami, które mogą być przeszukiwane i przetwarzane. • Automatyczne mechanizmy korelacji zdarzeń i stale rozwijany zestaw reguł korelacyjnych opartych między innymi na macierzy MITRE ATT&CK. • Silnik korelacyjny wyposażony w zestaw możliwości: <ol style="list-style-type: none"> i. Tworzenie zdarzeń na podstawie innych zdarzeń; ii. Tworzenie incydentów na podstawie zdarzeń; iii. Nadawanie priorytetów w zależności od kontekstu; iv. Mechanizm scoringowy uzależniony od profili zasobów; v. Tworzenie i odwoływanie się do tablic referencyjnych; vi. Uwzględnianie w korelacji kontekstu zasobów związanych ze zdarzeniami (typ zasobu i jego rola w organizacji, zagrożone procesy vii. techniczne i biznesowe, rodzaj przetwarzanych danych, potencjalne konsekwencje incydentu, wektory ataku, wyniki analizy viii. ryzyka); ix. Graficzny interfejs do tworzenia reguł korelacji;
26. Możliwość definiowania reguł analizy incydentów dla każdego odbieranego zdarzenia. Reguły winny umożliwiać korelację informacji technicznych wyciągniętych ze zdarzenia przekazanego z innych systemów (m.in. adres IP, kategoria, severity) z parametrami zdefiniowanymi w elektronicznej dokumentacji (m.in. ważność zasobu, klasyfikowane informacje, procesy organizacji) oraz aktualnymi incydentami bezpieczeństwa.
27. Detekcję anomalii poprzez osiągnięcie określonej liczby punktów na danym zasobie wliczonych z sumy punktów wszystkich zdarzeń na nim występujących w określonym przedziale czasu. W tym celu wynik działania reguł korelacyjnych winien być oceniany w skali punktowej, w odniesieniu do rodzaju zasobu oraz jego parametrów. Przykładowo to samo zdarzenie winno być inaczej oceniane jeżeli będzie dotyczyło komputera a inaczej jeżeli będzie miało miejsce na serwerze usług.
28. Możliwość budowania profili aktywności użytkowników oraz zasobów poprzez wielowartościowe listy referencyjne przykładowo: nazwa użytkownika, aplikacja i adres docelowy oraz umożliwiać wykorzystywanie ich w regułach korelacyjnych.
29. Priorytetyzowanie wykrytych incydentów w odniesieniu do ważności dla organizacji zasobów których dotyczą (tzn. wspomaganym procesów, przetwarzanych informacji klasyfikowanych). System winien udostępnić graficzny edytor pozwalający na dostosowanie reguł wyznaczania priorytetów obsługi względem dowolnych parametrów zawartych w elektronicznej dokumentacji;
30. Automatyczne wyznaczanie, dla zarejestrowanych incydentów, ścieżki ataku i prezentowanie jej w formie graficznej na schemacie sieci. Ścieżka ataku winna pokazywać wszystkie urządzenia zabezpieczeń na drodze pomiędzy sprawcą i ofiarą ataku.

31. Zaimplementowany proces zarządzania incydentami odbywający się etapowo, zgodnie z obowiązującymi standardami (m.in. ISO/IEC 27035)
32. Integrację narzędzi i zewnętrznych źródeł danych (w tym Threat Intelligence)
33. Automatyczne powiadomianie, w przypadku wykrycia incydentów o poważnych konsekwencjach dla organizacji , o zdarzeniu wskazanych pracowników, m.in. za pomocą email i SMS.
34. Prezentację podsumowania aktualnego stanu bezpieczeństwa w formie graficznej , m.in. procesy organizacji zagrożone przez incydenty bezpieczeństwa.
35. Prezentację danych w postaci tzw. „Dashboard” czyli dostosowanego zakresu i prezentacji danych do potrzeb administratora czy też zalogowanego użytkownika/operatora
36. Raportowania nt. krytycznych incydentów i podatności z możliwością eksportu do formatu PDF tudzież Kreator raportów.
37. Możliwość automatyzacji zadań analizy i reakcji na incydenty - Przebieg prac winien odbywać się zgodnie ze scenariuszami dostosowanymi do każdego etapu procesu obsługi incydentu. Proces obsługi incydentu winien być realizowany wg standardów i najlepszych praktyk (między innymi: ISO/IEC-270035, NIST SP 800-61R2, ENISA, Carnegie Mellon University)
38. Możliwość definiowania scenariuszy obsługi incydentów uruchamianych na podstawie następujących kryteriów: <ul style="list-style-type: none"> • w przypadku gdy zasób przetwarza zdefiniowane informacje klasyfikowane (np. dane osobowe), • w przypadku gdy zasób jest elementem określonego procesu organizacji, • w przypadku gdy zasób zlokalizowany jest w danej lokalizacji, • w przypadku gdy na zasobie może dojść do określonego cyberzagrożenia; • w przypadku gdy na zasobie może dojść do określonej konsekwencji naruszenia bezpieczeństwa; • w przypadku gdy na zasobie jest zainstalowany określony system operacyjny lub oprogramowanie • itp.
39. Scenariusze obsługi incydentów wraz z wykonaniem przykładowych akcji i powiązaniem ich z poszczególnymi krokami, w tym: <ul style="list-style-type: none"> • zmianę operatora; • zmianę statusu; • zmianę priorytetu; • przekazywanie i pobieranie parametrów z innych systemów poprzez skrypty SSH/PowerShell oraz REST API); • wysłanie powiadomień; • aktualizację dokumentów wraz z ich automatycznym wersjonowaniem; • gromadzenie informacji na bazie podręcznego schowka oraz dołączenia plików wraz z wyliczaniem dla nich funkcji skrótów; • aktualizację list referencyjnych; • edycję bazy wiedzy zarówno w kontekście określonego wątku jak i definiowania nowych; • założenie zadania;
40. Możliwość konfiguracji systemu, w ramach której przebieg procesu dostosuje się dynamicznie do pozyskanych w ramach jego obsługi informacji, umożliwiając następujące przykładowe funkcjonalności: <ul style="list-style-type: none"> • Automatyzację wykonania wielu kroków nie wymagających reakcji operatora; • Warunkowe wykonywanie kroków w zależności od informacji zawartej zarówno w elektronicznej dokumentacji jak i informacji pozyskanej z innych systemów; • Warunkowe wykonywanie kroków w zależności od odpowiedzi operatora na zdefiniowane pytanie;
41. Gotową integrację z producentami narzędzi do skanowania podatności (tzn. narzędzi Vulnerability Assessment) oraz CVE.
42. Możliwość definiowania harmonogramów skanowania podatności oraz na ich podstawie automatyczne uruchamianie procesów skanowania i analizy uzyskanych raportów.
43. Mechanizmy pozwalające na identyfikowanie komputerów na podstawie ich nazw, pozwalając tym samym na procesowanie podatności danego komputera nawet przy dynamicznym adresie IP pobieranym z serwera DHCP.

<p>44. Możliwość definiowania scenariuszy obsługi podatności uruchamianych na podstawie przykładowych kryteriów:</p> <ul style="list-style-type: none"> • w przypadku gdy zasób przetwarza zdefiniowane informacje klasyfikowane (np. dane osobowe), • w przypadku gdy zasób jest elementem określonego procesu organizacji, • w przypadku gdy zasób zlokalizowany jest w danej lokalizacji, • w przypadku gdy na zasobie może dojść do określonego cyberzagrożenia; • w przypadku gdy na zasobie może dojść do określonej konsekwencji naruszenia bezpieczeństwa; • w przypadku gdy na zasobie jest zainstalowany określony system operacyjny lub oprogramowanie
<p>45. Funkcjonalność automatycznego proponowania odpowiednich scenariuszy obsługi podatności. Scenariusze obsługi zawierać winny możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.</p>
<p>46. Automatyczne powiadamianie, w przypadku wykrycia podatności o poważnych konsekwencjach dla organizacji, o zdarzeniu wskazanych pracowników, m.in. za pomocą email i SMS.</p>
<p>47. Możliwość automatycznego przydzielania odpowiedniego zespołu obsługi dla danego zdarzenia w razie wykrycia podatności, na podstawie informacji wyciągniętej z wyniku skanu (np.: przedzielenie osób dla podatności dotyczących oprogramowania Microsoft SQL Server). Podczas procesu przydzielania podatności dla zespołów obsługi system winien brać pod uwagę ilość aktualnie obsługiwanych podatności przez członków zespołów (osobom które miałyby mniejszą ilość podatności przypisywane byłyby w pierwszej kolejności nowe podatności, w dalszej kolejności byłyby one rozkładane pomiędzy osobami równomiernie).</p>
<p>48. Możliwość tworzenia własnych wymagań bezpieczeństwa oraz ich weryfikacji względem zasobów IT w tym (serwerów, stacji roboczych oraz urządzeń sieciowych) na bazie RestAPI skryptów PowerShell/SSH oraz parametrów elektronicznej dokumentacji. System umożliwić winien rozbudowę list zgodności o wyniki działania przynajmniej jednego skanera podatności umożliwiającego przeprowadzenie skanowania typu COMPLIANCE.</p>
<p>49. Możliwość budowanie grupy wymagań dotyczących zgodności z normami czy rozporządzeniami (np.: Rekomendacja D czy PCS-DSS) pozwalając wpisać do systemu poszczególne wymagania (np.: punkty normy) oraz połączyć te wymagania ze skryptami je weryfikującymi. System winien pozwalać na automatyczne zbudowanie raportu zgodności na podstawie wyników skryptów weryfikujących oraz innych parametrów elektronicznej dokumentacji.</p>
<p>50. Możliwość analizy poprawności konfiguracji poszczególnych elementów systemu teleinformatycznego np.: przełączniki, systemy Firewall, serwery.</p>
<p>ZAKRES I WYTYCZNE PROCESU WDROŻENIA SYSTEMU PRZEZ WYKONAWCĘ</p>
<p>51. Proces wdrożenia systemu powinien zostać zrealizowany zgodnie z opisanymi niżej wytycznymi, umożliwiając efektywne wdrożenie rozwiązania w okresie 5 miesięcy.</p>
<p>52. Proces wdrożeniowy winien obejmować 3 obszary:</p> <ul style="list-style-type: none"> • Obszar Analizy, zakładający stworzenie elektronicznej dokumentacji organizacji wraz z podłączeniem i skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji (budowa kontekstu organizacji); <ul style="list-style-type: none"> i. Obszar Analizy ma na celu identyfikację potencjalnych cyberzagrożeń oraz możliwych konsekwencji na jakie narażona jest organizacja. Zakres prac powinien uwzględniać kolejno: <ol style="list-style-type: none"> 1. Zebranie przez konsultantów niezbędnych informacji dotyczących infrastruktury Zamawiającego, 2. Uruchomienie systemu w infrastrukturze Zamawiającego, 3. Przekierowanie ruchu sieciowego na do uruchomionego systemu, 4. Prace związane z analizą transmisji sieciowej, 5. Prace związane z analizą podatności systemu Zamawiającego, w tym instalacja i podłączenie komercyjnego skanera podatności lub zainstalowanie i podłączenie skanera podatności typu open source,

6. Przygotowanie dynamicznego raportu audytowego w oparciu o dostępne w systemie narzędzia elektronicznej dokumentacji i szacowania ryzyka obejmującego analizę prawdopodobieństwa przełamania zabezpieczeń organizacji. Raport powinien zawierać:
 - a. zidentyfikowane zagrożenia oraz prawdopodobieństwo ich wystąpienia;
 - b. potencjalne wektory ataków dla wykrytych zagrożeń;
 - c. wizualizacja graficzna wykrytych źródeł zagrożeń oraz wektorów ataków;
 - d. rekomendacja zabezpieczeń;
 - e. zidentyfikowane zagrożenia związane z podatnościami oraz prawdopodobieństwo wykorzystania ich do przełamania zabezpieczeń;
 7. Prezentacja wraz z interpretacją i omówieniem wyników analizy.
- **Obszar Detekcji**, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów;
 - i. Obszar Detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń. Zakres prac powinien uwzględniać kolejno:
 1. Podłączenie (przekierowanie do systemu) źródeł zdarzeń i ich dalszą konfigurację. Kluczowe źródła danych to:
 - a. zapory sieciowe w punktach styku z siecią Internet,
 - b. sieciowe systemy bezpieczeństwa dedykowane do wykrywania incydentów bezpieczeństwa
 - c. centralne systemy, dedykowane do kontroli złośliwego oprogramowania na stacjach końcowych/Serwerach, umożliwiające wykrywanie aktywności złośliwego oprogramowania,
 - d. kontroler domenowy,
 - e. systemy detekcji anomalii w przepływach lub zdarzeniach,
 - f. w przypadku niestandardowych źródeł, winne być przygotowane przez Wykonawcę odpowiednie parsery, pozwalające na detekcję zgodną z wbudowanymi w system regułami korelacji;
 2. Prace związane z dostosowaniem zdarzeń do zasobów, których dotyczą,
 3. Uruchomienie reguł detekcji,
 4. Dostrojenie systemu, mające na celu dopasowanie czułości systemu do możliwości operacyjnych organizacji;
 - **Obszar Reakcji**, zakładający podłączenie i konfigurację mechanizmów wspomagających proces automatyzacji reakcji na wykryte zdarzenia, incydenty bezpieczeństwa i podatności;
 - i. Uruchomienie i dostrojenie mechanizmów automatyzacji w działaniach reagowania na wykryte zagrożenia bezpieczeństwa. Zakres prac powinien uwzględniać kolejno:
 1. Przygotowanie gotowych scenariuszy umożliwiających automatyzację prac związanych z wykrywanym zagrożeniem,
 2. Prace związane określeniem zespołów obsługi celem właściwej adresacji podatności oraz zdarzeń wymagających obsługi;

53. Konfiguracja mechanizmów powiadamiania.

POZOSTAŁE WYMAGANIA DLA WDRAŻANEGO SYSTEMU:

1. Wdrożenie dotyczy objęcia monitoringiem 150 urządzeń (adresów IP) wskazanych przez Zamawiającego.
2. System winien funkcjonować w środowisku wirtualnym Vmware.
 - Wraz z ofertą Zamawiający przedstawi niezbędne wymagania dla maszyn wirtualnych do prawidłowego funkcjonowania systemu.
3. Wszelkie licencje niezbędne do uruchomienia systemu dostarcza Wykonawca na swój koszt.
 - Wraz z ofertą Wykonawca przedstawi wykaz licencji niezbędnych do uruchomienia systemu,

- W przypadku konieczności zakupu licencji innych producentów winne one być nabyte bezpośrednio na konto Zamawiającego.
4. Wraz z ofertą, jako opcję, Wykonawca przedstawi propozycję wdrożenia komercyjnego skanera podatności w miejsce rozwiązania open source w integracji z wdrażanym systemem.
 - Wymagane jest podanie zasobów dla maszyn wirtualnych niezbędnych do uruchomienia tego skanera w zasobach środowiska wirtualnego Zamawiającego.
 5. Wykonawca wykaże, iż dysponuje na potrzeby wykonania wdrożenia dwoma osobami, inżynierami systemowymi, posiadającymi co najmniej wykształcenie wyższe i 2 letnie doświadczenie w postaci zrealizowanych projektów dotyczących instalacji konfiguracji oferowanego oprogramowania. Liczba lat doświadczenia będzie liczona jako suma okresów pracy/świadczenia usług w ww. roli.

TABELA NR 2 – świadczenie usług serwisowych przez Wykonawcę w zakresie oprogramowania określonego w Tabeli Nr 1

Warunki serwisu – wymagane pisemne oświadczenia:
<p>Wykonawca zagwarantuje, że przez okres miesięcy, począwszy od daty obustronnego podpisania protokołu odbioru systemu, obsługa systemu będzie wolna od wad podczas zwykłego użytkowania i będzie przebiegać zgodnie z dokumentacją Producenta w zakresie pracy Systemu oraz System dostarczony przez Wykonawcę nie będzie zawierać żadnego typu oprogramowania lub innych elementów uważanych za nieautoryzowane:</p> <ol style="list-style-type: none"> a) nieautoryzowany dostęp b) uszkodzenie c) wykasowanie wszelkiego rodzaju oprogramowania, danych lub urządzeń peryferyjnych <p>Wykonawca będzie również świadczył usługę Wsparcia technicznego przez okres 12 miesięcy od daty zakończenia prac wdrożeniowych. W ramach usługi Wsparcia udostępnione zostaną Zamawiającemu nowe wersje oprogramowania (aktualizacje) obejmujące nowe funkcjonalności, o których Zamawiający zostanie powiadomiony drogą elektroniczną, i gdzie zostanie udostępniony link umożliwiający pobranie pakietu instalacyjnego wraz z instrukcją aktualizacji.</p> <p>Wsparcie techniczne dla systemu będzie obejmowało w szczególności:</p> <ul style="list-style-type: none"> - zapewnienie przez Wykonawcę kanały komunikacji pomiędzy Wykonawcą, a Zamawiającym, odpowiadająca za bieżącą obsługę systemu, rozwiązywanie prostych wniosków o usługę i nadzorująca przepływ zgłoszeń bez limitu czasowego, - zapewnienie przez Wykonawcę dedykowanego zespołu, posiadającego szerszą znajomość usług, pozwalających na działanie systemu (systemy operacyjne, bazy danych) oraz wiedzę w zakresie szczegółowej konfiguracji systemu wraz z pakietem godzin serwisowych. - o ile Wykonawca nie jest producentem systemu, zapewnienie przez Wykonawcę nieograniczonego czasowo kanału komunikacji świadczenia usług przez Producenta systemu, odpowiadających za pomoc techniczną w zakresie zgłoszeń, związanych z wykrytymi przez Zamawiającego błędami systemowymi. Ta linia wsparcia winna być świadczona w dni robocze, tj. od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy w godzinach od 8.00 do 16.00 i obejmować usuwanie awarii/ustererek/błędów w sposób umożliwiający funkcjonowanie Systemu, bądź jego elementu, zgodnie z przeznaczeniem i przywrócenie stanu sprzed awarii bądź, o ile zaistnieje taka potrzeba, stanu takiego jakby awarii w ogóle nie było. Naprawa ma na celu umożliwienie Zamawiającemu korzystanie z Systemu zgodnie z jego przeznaczeniem i właściwościami o niezmienionej wydajności. Czas usunięcia awarii/usterki/błędu nie może być dłuższy niż 48 godzin od zgłoszenia. Wykonawca musi wskazać nr kontaktowy oraz mail (lub stronę internetową CRM) służący do wysyłania zgłoszeń. - wymóg czasu reakcji Wykonawcy na zgłoszenia awarii o charakterze krytycznym (określenie charakteru awarii należy do Zamawiającego) dla funkcjonowania przedsiębiorstwa, łącznie z przybyciem wykwalifikowanego inżyniera, legitymującego się stosownymi uprawnieniami, do siedziby Zamawiającego – 8 godzin. - Wykonawca będzie przyjmował zgłoszenia serwisowe w dni robocze, w godzinach od 8:00 do 18:00 określając uprzednio serwisowe numery telefonów oraz adresy mailowe do osób odpowiedzialnych za wsparcie techniczne dla wdrażanego systemu.

Wykonawca akceptuje fakt, że prace serwisowe prowadzone będą na pracującym środowisku, z wymaganiem każdorazowego dopuszczenia Wykonawcy przez Zamawiającego do wykonania tych prac. Wykonawca musi mieć na uwadze, że system pracuje w trybie ciągłym z niewielkimi przerwami pomiędzy normalną pracą i zadaniami backupu oraz replikacji danych.

TABELA NR 3 – pozostałe wymagania

Pozostałe wymagania – wymagane pisemne oświadczenia:
Wykonawca dostarczy pisemne oświadczenie producenta systemu o możliwości uzyskania kodów źródłowych wraz z przyznaniem do nich praw Zamawiającemu w przypadku wystąpienia sytuacji szczególnej, związanej z zakończeniem działalności i nie scedowaniem praw na inny podmiot kontynuujący działalność w tym zakresie.
Wykonawca przeprowadzi szkolenie z obsługi i administracji wdrożonym systemem dla wskazanej przez Zamawiającego grupy operatorów / administratorów, w obustronnie uzgodnionym terminie. Minimalny czas trwania szkolenia: 3 dni robocze.
Wraz ze zgłoszeniem przystąpienia do odbioru końcowego systemu Wykonawca dostarczy pełną dokumentację techniczną systemu, w formie elektronicznej, wraz z instrukcjami jego obsługi w podziale na: - dokumentacja techniczna - instrukcja obsługi dla operatora - instrukcja obsługi dla administratora
Wraz ze zgłoszeniem przystąpienia do odbioru końcowego systemu Wykonawca dostarczy dokument poświadczający udzielenie miesięcznej gwarancji, wsparcia technicznego oraz wszystkie niezbędne licencje potwierdzające zgodne z prawem nabycie systemu przez Zamawiającego.
Zakończenie wdrożenia systemu winno być udokumentowane raportem końcowym z przeglądu cyberzagrożeń systemu teleinformatycznego przedsiębiorstwa.

Zamawiający zastrzega obowiązek osobistego wykonania przez wykonawcę kluczowych części zamówienia. Powyższe dotyczy: zapisów określonych w punkcie I. OPIS PRZEDMIOTU ZAMÓWIENIA, Tabele Nr 1 i 2.

Zamawiający nie dopuszcza składanie ofert częściowych.

II. TERMIN WYKONANIA PRZEDMIOTU ZAMÓWIENIA: 5 miesięcy od dnia podpisania umowy.

III. WARUNKI UDZIAŁU W POSTĘPOWANIU JAKIE MUSZĄ SPEŁNIAĆ WYKONAWCY, WYKLUCZENIE Z POSTĘPOWANIA

1. O udzielenie zamówienia mogą ubiegać się podmioty które spełniają następujące warunki udziału w postępowaniu :

- a. posiadają kompetencje lub uprawnienia do prowadzenia określonej działalności zawodowej związanej z wykonaniem przedmiotowego zamówienia, o ile konieczność ich posiadania wynika z odrębnych przepisów;
Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie Wykonawca zobowiązany jest wykazać w sposób szczególny. Zamawiający uzna, że powyższy warunek jest spełniony, jeżeli Wykonawca złoży oświadczenie (według wzoru stanowiącego Załącznik nr 2 do ogłoszenia/ specyfikacji) o spełnianiu tego warunku udziału w postępowaniu.
- b. posiadają zdolność techniczną lub zawodową niezbędną do należytego wykonania przedmiotowego zamówienia;

Zamawiający uzna niniejszy warunek za spełniony jeżeli Wykonawca przedstawi przynajmniej jedną referencję (potwierdzoną za zgodność z oryginałem) wdrożenia lub serwisowania środowiska teleinformatycznego, która co do zakresu (serwery, macierze, sieć SAN, system backupu, środowisko wirtualne, usługi katalogowe) pokrywa się z przedmiotem niniejszego postępowania, wykonanego w okresie ostatnich 3 lat przed upływem terminu składania ofert. Dowody to: referencje, protokoły odbioru, umowy. Jeżeli prace były wykonywane na rzecz Wodociągów Białostockich Sp. z o.o. to wystarczy wskazanie projektu i terminu).

- c. znajdują się w sytuacji ekonomicznej lub finansowej pozwalającej na należyte wykonanie przedmiotowego zamówienia.

Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnienie Wykonawca zobowiązany jest wykazać w sposób szczególny. Zamawiający uzna, że powyższy warunek jest spełniony, jeżeli Wykonawca złoży oświadczenie (według wzoru stanowiącego Załącznik nr 2 do ogłoszenia/ specyfikacji) o spełnianiu tego warunku udziału w postępowaniu.

2. Ponadto Wykonawcy ubiegający się o udzielenie przedmiotowego zamówienia nie mogą podlegać wykluczeniu z postępowania. Przesłanki skutkujące wykluczeniem z postępowania danego wykonawcy zostały szczegółowo określone w § 13 w/w Regulaminu. Oferta wykonawcy wykluczonego z postępowania uznana zostanie za odrzuconą.
3. W celu spełnienia warunków o których mowa powyżej oraz wykazaniu braku podstaw do wykluczenia, Wykonawcy winni przedłożyć następujące dokumenty:
 - 1) Odpis z właściwego rejestru (np. KRS lub wydruk z Centralnej Ewidencji i Informacji o Działalności Gospodarczej), jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;
 - 2) Formularz ofertowy, sporządzony na podstawie wzoru – **zał. Nr 1** do niniejszego Ogłoszenia/SIWZ;
 - 3) Oświadczenie wykonawcy, że spełnia warunki udziału w postępowaniu oraz że nie podlega wykluczeniu z postępowania zgodnie ze wzorem **zał. Nr 2** do Ogłoszenia/SIWZ;
 - 4) Pisemną akceptację, iż Oferent akceptuje fakt, że prace serwisowe prowadzone będą na pracującym środowisku, z wymaganiem każdorazowego dopuszczenia Wykonawcy przez Zamawiającego do wykonania tych prac. Wykonawca musi mieć na uwadze, że system pracuje w trybie ciągłym z niewielkimi przerwami pomiędzy normalną pracą i zadaniami backupu oraz replikacji danych (Formularz oferty pkt 4.6)
 - 5) Potwierdzenie wdrożenia zgodnie z punktem III.1.b

IV. INFORMACJE DOTYCZĄCE SPOSOBU PRZYGOTOWANIA OFERTY/ INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIU OŚWIADCZEŃ I DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI:

1. Wykonawca ma prawo złożyć tylko jedną ofertę.
2. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.
3. **Oferta powinna być sporządzona w formie pisemnej pod rygorem nieważności**, w języku polskim, na maszynie, komputerze lub czytelnym pismem ręcznym (długopisem lub nieścieralnym atramentem). Wszystkie dokumenty i oświadczenia w języku obcym winny być przetłumaczone na język polski. **UWAGA: Do oferty w formie pisemnej należy dołączyć skan oferty z załącznikami na nośniku elektronicznym.**
4. W przypadku składania dokumentów w formie kopii, winne być one potwierdzone za zgodność z oryginałem przez osoby uprawnione do reprezentowania Wykonawcy.
5. Wszystkie strony oferty, w tym strony wszystkich załączników, powinny być trwale spięte, ponumerowane, ułożone wg dołączonego spisu treści.
6. Ofertę podpisuje osoba/osoby uprawnione do reprezentowania Wykonawcy.
7. Wszystkie miejsca, w których wykonawca naniósł zmiany muszą być parafowane przez osobę/osoby uprawnione do reprezentowania Wykonawcy.
8. Oferta jest jawna z wyjątkiem informacji co do których dany wykonawca zastrzegł nie później jednak niż w terminie składania ofert, że nie mogą być one udostępniane gdyż stanowią one tajemnicę

przedsiębiorstwa w rozumieniu przepisów z art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993r. o zwalczaniu nieuczciwej konkurencji – (t.j. Dz. U. z 2019 r. poz. 1010 z późn. zm.) oraz wykazał, iż zastrzeżone informacje tajemnicę przedsiębiorstwa rzeczywiście stanowią.

9. Informacje stanowiące tajemnicę przedsiębiorstwa winny być zgrupowane i stanowić oddzielną część oferty, opisaną klauzulą „Tajemnica przedsiębiorstwa - tylko do wglądu przez Zamawiającego”.
10. Wszelkie oświadczenia, wnioski, zawiadomienia, wyjaśnienia oraz inne dokumenty (np. protest), jak i odpowiedzi na nie, przekazywane Zamawiającemu przez Wykonawców jak i Wykonawcom przez Zamawiającego, winny dla swej ważności mieć formę pisemną. Zamawiający dopuszcza porozumiewanie się za pomocą faksu lub e-mail pod warunkiem niezwłocznego potwierdzenia treści faksu, e - maila pismem.

Faks Zamawiającego - 85 / 74 58 113

Email Zamawiającego - przetargi@wobi.pl

11. Osobami uprawnionymi przez Zamawiającego do kontaktu z Wykonawcami są :
 - Robert Skrzymowski tel. 85 / 74 58 151 - sprawy merytoryczne
 - Jerzy Rusiłowicz tel. 85 / 74 58 136 - sprawy proceduralne

V. KRYTERIUM OCENY OFERT I SPOSÓB DOKONYWANIA WYBORU

1. Cena 80%
2. Doświadczenie 10 pkt
3. Gwarancja 5 pkt
4. Świadczenie usług wsparcia technicznego 5 pkt

Ad. 1. Ceny w ofercie przetargowej wpisane do formularza ofertowego (**Załącznik Nr 1 do SIWZ**) muszą obejmować wszystkie koszty oraz zobowiązania publicznoprawne jak i zastosowane rabaty i upusty finansowe. Powinny być podana jako wartości brutto i netto, ceny należy podać w zaokrągleniu do dwóch miejsc po przecinku. Jeżeli Wykonawca zaproponuje w ofercie rabaty lub upusty nie uwzględnione w cenie wpisanej do formularza ofertowego Zamawiający nie będzie ich brał pod uwagę przy ocenie oferty.

Ocena punktowa kryterium będzie obliczana wg następującej formuły:

$$\text{Ocena oferty X} = \frac{\text{Wartość brutto oferty najtańszej w danym zadaniu}}{\text{Wartość brutto oferty ocenianej w danym zadaniu}} \times 80 \%$$

UWAGA: Zamawiający może wezwać Wykonawcę, którego oferta okaże się w postępowaniu przetargowym najkorzystniejsza do udzielenia pisemnych wyjaśnień, w tym złożenie dowodów, dotyczących elementów oferty mających wpływ na wysokość ceny (kosztu),

Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny, spoczywa na Wykonawcy.

Zamawiający odrzuci ofertę Wykonawcy, który w wyznaczonym przez Zamawiającego terminie nie złoży wyjaśnień (wraz z dowodami) lub jeżeli dokonana ocena wyjaśnień (wraz z dostarczonymi dowodami) potwierdzi, że oferta zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia. W związku z powyższym zaleca się zachowanie należytej staranności przy kalkulacji ceny oferty oraz zachowanie pisemnych dowodów /np. ofert, umów, faktur/ dotyczących kalkulacji ceny (kosztu) oferty.

Ad. 2. Kryterium „Doświadczenie”: dołączyć do oferty referencje potwierdzone za zgodność z oryginałem dla maksymalnie 5 wdrożeń lub usług serwisowych, które co do zakresu pokrywają się z przedmiotem oferty określonym w Tabeli Nr 1. Dowody to: referencje, protokoły, jeżeli prace były

wykonywane na rzecz Wodociągów Białostockich Sp. z o.o. to tylko wskazanie projektu i terminu). Pod uwagę będą brane referencje, których data realizacji przypadła na lata 2016 - 2020. Każda potwierdzona referencja, zgodna z powyższymi założeniami to 2 pkt.

Łącznie do uzyskania w kryterium „Doświadczenie”: 10 punktów.

UWAGA: Do punktacji nie uwzględnia się doświadczenia podanego w ramach spełnienia warunku udziału w postępowaniu III.1.b).

Ad.3. Kryterium „Gwarancja”: Maksymalna ilość punktów jaką można uzyskać:

Gwarancja (12 m-cy)	– 0 pkt.
Gwarancja (24 miesiące)	– 2 pkt.
Gwarancja(36 miesięcy)	– 5 pkt.

Łącznie do uzyskania w kryterium „Gwarancja” i autoryzacje: 5 pkt w danej części.

Ad.4. Kryterium „Świadczenie usług wsparcia technicznego”: Maksymalna ilość punktów jaką można uzyskać w okresie świadczenia gwarancji:

Pakiet 50 godzin serwisowych rocznie	– 0 pkt.
Pakiet 100 godzin serwisowych rocznie	– 2 pkt.
Pakiet 200 godzin serwisowych rocznie	– 5 pkt.

Dotyczy zapewnienie przez Wykonawcę dedykowanego zespołu, posiadającego szerszą znajomość usług, pozwalających na działanie systemu (systemy operacyjne, bazy danych) oraz wiedzę w zakresie szczegółowej konfiguracji systemu.

Łącznie do uzyskania w kryterium „Świadczenie usług wsparcia technicznego”: 5 pkt w danej części.

Za najkorzystniejszą uznana zostanie oferta, która uzyska łączną, najwyższą liczbę punktów ze wszystkich w/w kryteriów.

Zamawiający udzieli zamówienia Wykonawcom, których oferty odpowiadają wszystkim wymaganiom zawartym w SIWZ i zostały ocenione jako najkorzystniejsze w danym zadaniu.

VI. WADIUM

Zamawiający nie wymaga od wykonawców wniesienia wadium.

VII. ZABEZPIECZENIE NALEŻYTEGO WYKONANIA UMOWY

Zamawiający nie wymaga od Wykonawców wniesienia zabezpieczenia należytego wykonania umowy.

VIII. FORMALNOŚCI JAKIE POWINNY ZOSTAĆ DOPEŁNIONE W CELU ZAWARCIA UMOWY

Zamawiający niezwłocznie powiadomi wszystkich Wykonawców, którzy złożyli oferty podając nazwę firmy, siedzibę oraz ceny, a wybranemu Wykonawcy wskaże termin i miejsce podpisania umowy.

IX. MIEJSCE I TERMIN SKŁADANIA ORAZ OTWARCIA OFERT

Ofertę należy złożyć w Sekretariacie Wodociągów Białostockich Spółka z o.o. w Białymstoku, ul. Młynowa 52/1 **do dnia 10 lipca 2020 r. do godz. 13⁰⁰**

Oferta powinna być złożona u Zamawiającego w zamkniętej kopercie opisanej w następujący sposób:

„Wodociągi Białostockie Sp. z o.o. 15-404 Białystok, ul. Młynowa 52/1”

z dopiskiem

„Oferta na

„Przeгляdu cyberzagrożeń przedsiębiorstwa - NI-I-3/2020”

Nie otwierać przed dniem 10 lipca 2020 r. do godz. 13¹⁵”;

oraz nazwą Wykonawcy.

Publiczne otwarcie ofert nastąpi w siedzibie Zamawiającego - Białystok, ul. Młynowa 52/1 **w dniu 10 lipca 2020 r. do godz. 13¹⁵ świetlica.**

X. TERMIN ZWIĄZANIA OFERTA

1. Termin związania ofertą wynosi 45 dni i liczony jest od dnia w którym upływa termin składania ofert.

XI. INFORMACJE O PRZEWIDYWANYCH ZAMÓWIENIACH UZUPEŁNIAJĄCYCH

Zamawiający nie przewiduje udzielenia zamówień uzupełniających o których mowa w § 34 ust. 1 pkt. 6 i 7 Regulaminu.

XII. PROTEST

1. Jeżeli Zamawiający w procesie udzielania zamówienia naruszy w sposób wyraźny i bezpośredni ustalone przez siebie w niniejszym *Regulaminie*, Specyfikacji Istotnych Warunków Zamówienia lub Ogłoszenia zasady udzielania zamówienia, Wykonawcy przysługuje prawo do złożenia pisemnego, uzasadnionego protestu do Zamawiającego.
2. Protest o którym mowa w ust. 1 przysługuje tylko i wyłącznie w zakresie naruszenia dotyczącego
 - a. opisu przedmiotu zamówienia,
 - b. opisu kryteriów oceny ofert,
 - c. odrzucenia oferty protestującego lub wykluczenia go z postępowania,
 - d. wyboru oferty najkorzystniejszej.
3. Protest powinien wskazywać czynność lub zaniechanie czynności **Zamawiającego**, której zarzuca się niezgodność z *Regulaminem*, Specyfikacją Istotnych Warunków Zamówienia lub Ogłoszenia, zawierać związane przedstawienie zarzutów, określać żądanie oraz wskazywać okoliczności faktyczne i prawne uzasadniające jego wniesienie.
4. Protest wnosi się w terminie 5 dni licząc od daty w jakiej wykonawca dowiedział się lub mógł dowiedzieć przy dołożeniu należytej staranności o czynności lub zaniechaniu zamawiającego w zakresie o którym jest mowa w ust. 1 i 2.
5. Zamawiający rozpatruje protest niezwłocznie z tym, że zastrzega sobie prawo do nie ustosunkowania się do wniesionego protestu w sytuacji gdy uzna go za niezasadny.
6. Wniesienie protestu nie wstrzymuje biegu postępowania ani też dokonania jego rozstrzygnięcia (wyboru oferty najkorzystniejszej lub unieważnienia postępowania) czy też podpisania umowy.

XIII. WYJAŚNIENIA TREŚCI OGŁOSZENIA ORAZ SIWZ

1. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści Specyfikacji Istotnych Warunków Zamówienia lub Ogłoszenia.

Uwaga: pożądane jest złożenie zapytania w wersji edytowalnej.

2. Zamawiający udzieli wyjaśnienia pod warunkiem że wniosek o wyjaśnienie treści Specyfikacji Istotnych Warunków Zamówienia lub Ogłoszenia wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. W innym wypadku Zamawiający uznając wniosek Wykonawcy za zasadny może udzielić wyjaśnienia.
3. Treść wniosku Wykonawcy wraz z udzielonymi wyjaśnieniami Zamawiający zamieszcza na stronie internetowej bip.wobi.pl bez ujawnienia źródła zapytania w terminie nie dłuższym niż na 4 dni przed wyznaczonym terminem na składanie ofert.
4. W uzasadnionych przypadkach Zamawiający może w każdym czasie przed upływem terminu składania ofert zmienić treść Specyfikacji Istotnych Warunków Zamówienia lub/i Ogłoszenia. Zmianę treści Specyfikacji Istotnych Warunków Zamówienia i/lub Ogłoszenia, Zamawiający zamieszcza niezwłocznie na stronie internetowej bip.wobi.pl.
5. Zamawiający przedłuża termin składania ofert, jeżeli w wyniku zmiany treści Specyfikacji Istotnych Warunków Zamówienia lub Ogłoszenia niezbędny jest dodatkowy czas na uwzględnienie wprowadzonych zmian w treści składanych ofert lub dołączanych do ofert dokumentów.

Zamawiający zastrzega sobie prawo zamknięcia przetargu bez wyboru którejkolwiek z ofert.

O unieważnieniu przetargu albo zamknięciu postępowania bez wyboru którejkolwiek z ofert Zamawiający poinformuje wszystkich Wykonawców którzy złożyli oferty. Dodatkowo informacje te zamieści na stronie internetowej bip.wobi.pl, oraz na tablicy ogłoszeń w swojej siedzibie.

W SPRAWACH NIEUREGULOWANYCH W SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA ZASTOSOWANIE MAJĄ ZAPISY W/W REGULAMINU ORAZ PRZEPISY KODEKSU CYWILNEGO.

Załączniki:

- Załącznik Nr 1 – Formularz ofertowy
- Załącznik Nr 2 – Oświadczenie Wykonawcy, że spełnia warunki udziału w postępowaniu oraz nie podlega wykluczeniu z postępowania;
- Załącznik Nr 3 – Klauzula informacyjna z artykułem 13 RODO
- Załącznik Nr 4 – Wzór/Projekt umowy

Z poważaniem
PREZES ZARZĄDU WICEPREZES ZARZĄDU
Beata Wiśniewska
Beata Wiśniewska Jarosław Poniatowicz
podpis Zamawiającego

KIEROWNIK
DZIAŁU PRZETARGÓW

FORMULARZ OFERTY**Przeprowadzenie przeglądu cyberzagrożeń przedsiębiorstwa w oparciu o wdrożenie systemu typu GRC (Governance, Risk Management, Compliance - Ład Korporacyjny, Zarządzanie Ryzykiem, Zgodność)**

1. ZAMAWIAJĄCY:

„Wodociągi Białostockie” Sp. z o.o.

zarejestrowana w Sądzie Rejonowym w Białymstoku XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod Nr KRS 0000024985, NIP 542-020-01-22, kapitał zakładowy: 165 540 000,00 zł

Adres: ul. Młynowa 52/1
15-404 Białystok
Polska

tel. +48 85 74 58 100
fax +48 85 74 58 113
Adres internetowy: www.wobi.pl

2. WYKONAWCA:

Nazwa:.....
Siedziba:
Tel/Fax:
REGON:
NIP.....
Adres strony internetowej:

3. OSOBA UPRAWNIONA DO KONTAKTÓW:

Imię i nazwisko	
Adres	
Nr telefonu	
Nr faksu	

4. Ja (my) niżej podpisany(i) oświadczam(y), że:

- 1) Zapoznałem(liśmy) się z treścią Ogłoszenia/Specyfikacji Istotnych Warunków Zamówienia (SIWZ) wraz z załącznikami (w tym ze wzorem umowy) i nie wnosimy do nich żadnych zastrzeżeń ani uwag.
- 2) Gwarantuję(my) wykonanie przez w/w Wykonawcę całości przedmiotu zamówienia na warunkach określonych przez Zamawiającego w treści Ogłoszenia/Specyfikacji Istotnych Warunków Zamówienia (SIWZ) wraz z załącznikami przy uwzględnieniu wyjaśnień Zamawiającego.
- 3) Oświadczam/my, że wyceniliśmy wszystkie elementy niezbędne do prawidłowego wykonania zamówienia.
- 4) Akceptuję/my termin realizacji zamówienia wynoszący 5 miesięcy od dnia podpisania umowy.
- 5) Cena mojej (naszej) oferty za realizację niniejszego zamówienia dotyczy dostawy i usług, i wynosi:

PRZEDMIOT ZAMÓWIENIA – CENY ELEMENTÓW DOSTAWY I USŁUG

Przeprowadzenia przeglądu cyberzagrożeń przedsiębiorstwa w oparciu o wdrożenie systemu typu GRC (Governance, Risk Management, Compliance - Ład Korporacyjny, Zarządzanie Ryzykiem, Zgodność).

Cena:

Łączna wartość netto w PLN:
Słownie:
VAT 23%:
Słownie:
Łączna wartość brutto w PLN:
Słownie:

Doświadczenie:

Ilość referencji potwierdzonych za zgodność z oryginałem:

Gwarancja:

Długość okresu gwarancyjnego w miesiącach:
--

Świadczenie usług wsparcia technicznego:

Wielkość godzinowa pakietu serwisowego w skali roku:
--

Oświadczam/my, iż nasza oferta spełnia wszystkie parametry i wymagania wskazane w Rozdziale I Ogłoszenia / SIWZ oraz we wzorze Umowy.

6) Oświadczam, że usługi serwisowe będą świadczone według zapisów poniższej tabeli.

Warunki serwisu:
<p>Wykonawca zagwarantuje, że przez okres miesięcy, począwszy od daty obustronnego podpisania protokołu odbioru systemu, obsługa systemu będzie wolna od wad podczas zwykłego użytkowania i będzie przebiegać zgodnie z dokumentacją Producenta w zakresie pracy Systemu oraz System dostarczony przez Wykonawcę nie będzie zawierać żadnego typu oprogramowania lub innych elementów uważanych za nieautoryzowane:</p> <ul style="list-style-type: none"> a) nieautoryzowany dostęp b) uszkodzenie c) wykasowanie wszelkiego rodzaju oprogramowania, danych lub urządzeń peryferyjnych
<p>Wykonawca będzie również świadczył usługę Wsparcia technicznego przez okres 12 miesięcy od daty zakończenia prac wdrożeniowych. W ramach usługi Wsparcia udostępnione zostaną Zamawiającemu nowe wersje oprogramowania (aktualizacje) obejmujące nowe funkcjonalności, o których Zamawiający zostanie powiadomiony drogą elektroniczną, i gdzie zostanie udostępniony link umożliwiający pobranie pakietu instalacyjnego wraz z instrukcją aktualizacji.</p> <p>Wsparcie techniczne dla systemu będzie obejmowało w szczególności:</p> <ul style="list-style-type: none"> - zapewnienie przez Wykonawcę kanały komunikacji pomiędzy Wykonawcą, a Zamawiającym, odpowiadająca za bieżącą obsługę systemu, rozwiązywanie prostych wniosków o usługę i nadzorująca przepływ zgłoszeń bez limitu czasowego, - zapewnienie przez Wykonawcę dedykowanego zespołu, posiadającego szerszą znajomość usług, pozwalających na działanie systemu (systemy operacyjne, bazy danych) oraz wiedzę w zakresie szczegółowej konfiguracji systemu wraz z pakietem godzin serwisowych. - o ile Wykonawca nie jest producentem systemu, zapewnienie przez Wykonawcę nieograniczonego czasowo kanału komunikacji świadczenia usług przez Producenta systemu, odpowiadających za pomoc

R

techniczną w zakresie zgłoszeń, związanych z wykrytymi przez Zamawiającego błędami systemowymi. Ta linia wsparcia winna być świadczona w dni robocze, tj. od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy w godzinach od 8.00 do 16.00 i obejmować usuwanie awarii/usterek/błędów w sposób umożliwiający funkcjonowanie Systemu, bądź jego elementu, zgodnie z przeznaczeniem i przywrócenie stanu sprzed awarii bądź, o ile zaistnieje taka potrzeba, stanu takiego jakby awarii w ogóle nie było. Naprawa ma na celu umożliwienie Zamawiającemu korzystanie z Systemu zgodnie z jego przeznaczeniem i właściwościami o niezmienionej wydajności. Czas usunięcia awarii/usterek/błędu nie może być dłuższy niż 48 godzin od zgłoszenia. Wykonawca musi wskazać nr kontaktowy oraz mail (lub stronę internetową CRM) służący do wysyłania zgłoszeń.

- wymóg czasu reakcji Wykonawcy na zgłoszenia awarii o charakterze krytycznym (określenie charakteru awarii należy do Zamawiającego) dla funkcjonowania przedsiębiorstwa, łącznie z przybyciem wykwalifikowanego inżyniera, legitymującego się stosownymi uprawnieniami, do siedziby Zamawiającego – 8 godzin.

- Wykonawca będzie przyjmował zgłoszenia serwisowe w dni robocze, w godzinach od 8:00 do 18:00 określając uprzednio serwisowe numery telefonów oraz adresy mailowe do osób odpowiedzialnych za wsparcie techniczne dla wdrażanego systemu.

Wykonawca akceptuje fakt, że prace serwisowe prowadzone będą na pracującym środowisku, z wymaganiami każdorazowego dopuszczenia Wykonawcy przez Zamawiającego do wykonania tych prac. Wykonawca musi mieć na uwadze, że system pracuje w trybie ciągłym z niewielkimi przerwami pomiędzy normalną pracą i zadaniami backupu oraz replikacji danych.

- 7) Akceptuję/my bez zastrzeżeń warunki płatności określone w Ogłoszeniu/SIWZ.
- 8) Niniejsza oferta jest ważna przez okres 45 dni,
- 9) W przypadku uznania mojej (naszej) oferty za najkorzystniejszą zobowiązuje(emy) się zawrzeć umowę w miejscu i terminie jakie zostaną wskazane przez Zamawiającego.
- 10) Nie uczestniczę(my) jako Wykonawca w jakiegokolwiek innej ofercie złożonej w celu udzielenia niniejszego zamówienia.;
- 11) Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu. *(W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (przez jego wykreślenie).*
- 12) Wyrażam zgodę na przetwarzanie danych osobowych zgodnie z postanowieniami załącznika Nr 3 do niniejszego Ogłoszenia/ Specyfikacji Istotnych Warunków Zamówienia (SIWZ).
- 13) W ofercie *znajdują się/nie znajdują się informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu Ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2019 r. poz. 1010 z późn. zm.). Wskazane poniżej informacje zawarte w ofercie stanowią tajemnicę przedsiębiorstwa i w związku z niniejszym nie mogą być one udostępniane, w szczególności innym uczestnikom postępowania:

Lp.	Oznaczenie rodzaju (nazwy) informacji	Strony w ofercie (wyrażone cyfrą)	
		od	do

UZASADNIENIE:.....

..... dn.2020 r.

.....
(Pieczęć/cie i podpis/y)

* niepotrzebne skreślić

****** W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).

¹⁾ 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).

Załączniki do oferty:

1.
2.
3.
4.
5.

Q- *Burśmiewska*

Dotyczy: Przeprowadzenie przeglądu cyberzagrożeń przedsiębiorstwa w oparciu o wdrożenie systemu typu GRC (Governance, Risk Management, Compliance - Ład Korporacyjny, Zarządzanie Ryzykiem, Zgodność)

ZAMAWIAJĄCY:

**WODOCIĄGI BIAŁOSTOCKIE Sp. z o.o. w Białymstoku
15-404 Białystok, ul. Młynowa 52/1**

I.p.	Pełna nazwa Wykonawcy/ców	Adres Wykonawcy

OŚWIADCZENIE

o spełnianiu warunków udziału w postępowaniu oraz braku podstaw do wykluczenia

I. Działając w imieniu i na rzecz w/w Wykonawcy Ja (my) niżej podpisany(i) oświadczam(y), że w/w Wykonawca:

- 1) posiada odpowiednie kompetencje lub uprawnienia do prowadzenia określonej działalności zawodowej związanej z wykonaniem przedmiotowego zamówienia, o ile konieczność ich posiadania wynika z odrębnych przepisów;
- 2) posiada stosowną zdolność techniczną lub zawodową niezbędną do należytego wykonania przedmiotowego zamówienia;
- 3) znajduje się w odpowiedniej, określonej sytuacji ekonomicznej lub finansowej pozwalającej na należyte wykonanie przedmiotowego zamówienia.

Ponadto oświadczam/y że w/w Wykonawca nie podlega wykluczeniu z przedmiotowego postępowania na podstawie § 13 „Regulaminu udzielania zamówień sektorowych w sytuacji braku obowiązku stosowania przepisów ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych” w brzmieniu:

II.Z postępowania o udzielenie zamówienia wyklucza się:

- 1) wykonawcę w stosunku do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. - Prawo restrukturyzacyjne (Dz. U. poz. 978, z późn. zm.) lub którego upadłość ogłoszono, z wyjątkiem wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd

- zarządził likwidację jego majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. - Prawo upadłościowe (Dz. U. z 2015 r. poz. 233, z późn. zm.);
- 2) wykonawcę który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych, z wyjątkiem przypadku, o którym mowa w pkt 6), chyba że wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
 - 3) wykonawcę, który nie wykazał spełniania warunków udziału w postępowaniu lub nie został zaproszony do negocjacji lub złożenia ofert wstępnych albo ofert, lub nie wykazał braku podstaw wykluczenia;
 - 4) wykonawcę będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
 - a) o którym mowa w [art. 165a](#), [art. 181-188](#), [art. 189a](#), [art. 218-221](#), [art. 228-230a](#), [art. 250a](#), [art. 258](#) lub [art. 270-309](#) ustawy z dnia 6 czerwca 1997 r. - Kodeks karny (Dz. U. poz. 553, z późn. zm.) lub [art. 46](#) lub [art. 48](#) ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2016 r. poz. 176),
 - b) o charakterze terrorystycznym, o którym mowa w [art. 115 § 20](#) ustawy z dnia 6 czerwca 1997 r. - Kodeks karny,
 - c) skarbowe,
 - d) o którym mowa w [art. 9](#) lub [art. 10](#) ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769);
 - 5) wykonawcę, jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 4);
 - 6) wykonawcę, wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, chyba że wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
 - 7) wykonawcę, który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawieniu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub obiektywne i nie dyskryminacyjne kryteria, zwane dalej "kryteriami selekcji", lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych dokumentów;
 - 8) wykonawcę, który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd zamawiającego, mogące mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia;
 - 9) wykonawcę, który bezprawnie wpływał lub próbował wpłynąć na czynności zamawiającego lub pozyskać informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia;
 - 10) wykonawcę, który brał udział w przygotowaniu postępowania o udzielenie zamówienia lub którego pracownik, a także osoba wykonująca pracę na podstawie umowy zlecenia, o dzieło, agencyjnej lub innej umowy o świadczenie usług, brał udział w przygotowaniu takiego postępowania, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu;
 - 11) wykonawcę, który z innymi wykonawcami zawarł porozumienie mające na celu zakłócenie konkurencji między wykonawcami w postępowaniu o udzielenie zamówienia, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych;
 - 12) wykonawcę będącego podmiotem zbiorowym, wobec którego sąd orzekł zakaz ubiegania się o zamówienia publiczne na podstawie [ustawy](#) z dnia 28 października 2002 r.

2-

o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (Dz. U. z 2015 r. poz. 1212, 1844 i 1855 oraz z 2016 r. poz. 437 i 544);

- 13) *wykonawcę, wobec którego orzeczono tytułem środka zapobiegawczego zakaz ubiegania się o zamówienia publiczne.*
- 14) *wykonawcę który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych;*

Z postępowania o udzielenie zamówienia wyklucza się również wykonawców, którzy należąc do tej samej grupy kapitałowej, w rozumieniu [ustawy](#) z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2015 r. poz. 184, 1618 i 1634), złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że istniejące między nimi powiązania nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.

..... dn.....2020 r.

.....
(Pieczęć/cie i podpis/y)

Q - *Wisniewska*

Dot.: Przeprowadzenie przeglądu cyberzagrożeń przedsiębiorstwa w oparciu o wdrożenie systemu typu GRC (Governance, Risk Management, Compliance - Ład Korporacyjny, Zarządzanie Ryzykiem, Zgodność)

KLAUZULA INFORMACYJNA z art. 13 RODO

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, informuję, że:

- administratorem Pani/Pana danych osobowych są Wodociągi Białostockie Sp. z o.o. w Białymstoku, 15-404 Białystok, ul. Młynowa 52/1, tel. 85 74 58 113, fax: 85 74 58 113, e-mail; sekretariat @wobi.pl
- inspektorem ochrony danych osobowych w Wodociągach Białostockich Sp. z o.o. jest Pan Rafał Nalewajko, e-mail: rodo@wobi.pl i iodo@wobi.pl
- Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego,
- odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja
- Pani/Pana dane osobowe będą przechowywane, zgodnie § 58 ust 1 pkt 2 wyżej przywołanego Regulaminu t. j. przez okres 5 lat od końca roku w którym przedmiot umowy został wykonany albo 5 lat od dnia unieważnienia/ zamknięcia postępowania bez wyboru którejkolwiek z ofert;
- obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem wynikającym z zasady jawności postępowania;
- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- posiada Pani/Pan:
 - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
 - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych **;
 - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO ***;
 - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- nie przysługuje Pani/Panu:
 - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;

- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
- **na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.**

PREZES, ZARZĄDU

Beata Wiśniewska
Beata Wiśniewska

WICEPREZES ZARZĄDU

Jarosław Poniatowicz
Jarosław Poniatowicz

* **Wyjaśnienie:** informacja w tym zakresie jest wymagana, jeżeli w odniesieniu do danego administratora lub podmiotu przetwarzającego istnieje obowiązek wyznaczenia inspektora ochrony danych osobowych.

** **Wyjaśnienie:** skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania

o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.

*** **Wyjaśnienie:** prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

UMOWA NR 2 /NI/ 2020

zawarta w dniu r. w Białymstoku pomiędzy:

„Wodociągami Białostockimi” Sp. z o.o. w Białymstoku, 15 - 404 Białystok, ul. Młynowa 52/1, zarejestrowaną w Sądzie Rejonowym w Białymstoku, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod Nr KRS 0000024985, NIP 542-020-01-22, REGON 050207647, kapitał zakładowy 165 540 000, 00 zł, zwaną dalej **Zamawiającym**, w imieniu której działają:

1. Beatę Wiśniewską - Prezesa Zarządu,
2. Henryk Jakubowicz - Dyrektor Zakładu Produkcji i Eksploatacji, Prokurent;

a

....., ul., zarejestrowaną w
pod nr KRS, NIP, Regon

reprezentowanym przez:

1. -

zwanym dalej **Wykonawcą**,

Zamawiający i Wykonawca zwani są dalej łącznie **Stronami** lub oddzielnie **Stroną**.

W wyniku przeprowadzonego postępowania w trybie przetargu nieograniczonego na podstawie **Regulaminu udzielania zamówień sektorowych w sytuacji braku obowiązku stosowania przepisów ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych** obowiązującego w „Wodociągach Białostockich” Sp. z o.o. w Białymstoku, wprowadzonego w życie Uchwałą Nr 91/2016 Zarządu Wodociągów Białostockich Sp. z o.o. w Białymstoku z dnia 28 listopada 2016 r., zawarta została umowa następującej treści :

§ 1

Przedmiot Umowy

1. Przedmiotem Umowy jest **przeprowadzenie przeglądu cyberzagrożeń przedsiębiorstwa w oparciu o wdrożenie systemu typu GRC (Governance, Risk Management, Compliance - Ład Korporacyjny, Zarządzanie Ryzykiem, Zgodność)**:

Wykonawca:

- a) dostarczy i zainstaluje system typu GRC (Governance, Risk Management, Compliance - Ład Korporacyjny, Zarządzanie Ryzykiem, Zgodność), który obejmie swoim zasięgiem 150 urządzeń (adresów IP). Szczegółowy zakres rzeczowy określa SIWZ wraz z Opisem przedmiotu zamówienia, stanowiący **załącznik nr 1** do niniejszej Umowy. Wdrożony system zostanie wymieniony z nazwy w załączniku do faktury wystawionej przez **Wykonawcę** po podpisaniu protokołu odbioru końcowego,
- b) dostarczy i zainstaluje wszelkie licencje firm trzecich niezbędne do uruchomienia systemu wymienionego w punkcie a) z tym zastrzeżeniem, że będą one zakupione przez Wykonawcę bezpośrednio na rzecz Zamawiającego. Wdrożone licencje zostaną wymienione z nazwy w załączniku do faktury wystawionej przez **Wykonawcę** po podpisaniu protokołu odbioru końcowego,
- c) wdroży komercyjny skaner podatności w miejsce rozwiązania open source w integracji z wdrażanym systemem wymienionym w punkcie a), o ile **Zamawiający** zdecyduje się na to rozwiązanie. W takim przypadku system ten zostanie wymieniony z nazwy w załączniku do faktury wystawionej przez **Wykonawcę** po podpisaniu protokołu odbioru końcowego,
- d) przeprowadzi szkolenie z obsługi i administracji wdrożonym systemem dla wskazanej przez **Zamawiającego** grupy operatorów / administratorów, w obustronnie uzgodnionym terminie. Minimalny czas trwania szkolenia: 3 dni robocze.
- e) dostarczy wraz z dokumentem zgłoszenia systemu do obioru raport z przeglądu cyberzagrożeń przedsiębiorstwa, wykonany w oparciu o wdrożony system typu GRC, wymieniony w punkcie a) w formie papierowej i elektronicznej, w ilości 3 egzemplarzy dla każdej z wymienionych form.

- f) wraz ze zgłoszeniem przystąpienia do odbioru końcowego systemu Wykonawca dostarczy pełną dokumentację techniczną systemu, w formie elektronicznej i papierowej, w ilości 3 egzemplarzy dla każdej z wymienionych form, wraz z instrukcjami jego obsługi w podziale na:
- dokumentacja techniczna
 - instrukcja obsługi dla operatora
 - instrukcja obsługi dla administratora
2. **Strony** przed przystąpieniem do wykonywania przedmiotu zamówienia podpiszą umowę powierzenia przetwarzania danych osobowych, która będzie obowiązywała przez okres obowiązywania niniejszej Umowy, a także w okresie gwarancyjnym i sprawowania opieki serwisowej.

§ 2 Termin realizacji

Strony ustalają 5 miesięczny termin realizacji przedmiotu Umowy liczony od daty podpisania Umowy tj. do dnia

§ 3 Obowiązki Zamawiającego

Do obowiązków **Zamawiającego** należy:

1. Stała współpraca z **Wykonawcą** podczas realizacji przedmiotu Umowy,
2. Terminowe uregulowanie należności za usługę zrealizowaną przez **Wykonawcę**,
3. **Zamawiający** przygotuje i przekaze **Wykonawcy**:
 - Wzór umowy powierzenia przetwarzania danych osobowych do podpisania przez Strony przed przystąpieniem do wykonywania prac.

§ 4 Obowiązki Wykonawcy

Do obowiązków **Wykonawcy** należy :

1. Terminowe wykonanie i przekazanie **Zamawiającemu** przedmiotu Umowy.
2. Wykonanie przedmiotu Umowy zgodnie z SIWZ, ofertą Wykonawcy, ustaleniami, obowiązującymi przepisami, zasadami wiedzy technicznej.
3. Zapewnienie wykonania przedmiotu Umowy przez personel posiadający odpowiednie kwalifikacje, wiedzę i umiejętności.
4. Zachowanie wymaganej staranności i terminowości w trakcie wykonywania usługi będącej przedmiotem niniejszej umowy
5. Usuwanie w sposób terminowy i na wyłączny koszt **Wykonawcy** wad i usterek przedmiotu Umowy stwierdzonych w czasie trwania usługi, po ich zakończeniu, a także w okresie gwarancji i rękojmi.
6. Stała współpraca z **Zamawiającym** w zakresie realizacji przedmiotu Umowy.
7. Wykonanie zaleceń **Zamawiającego** w trakcie realizacji przedmiotu Umowy.
8. Pozostawanie odpowiedzialnym za przedmiot Umowy do czasu jego odbioru ostatecznego przez **Zamawiającego**.
9. **Wykonawca** zobowiązuje się wykonać wszelkie prace dodatkowe, zamiennie i uzupełniające wskazane przez **Zamawiającego** zmierzające do prawidłowego zrealizowania przedmiotu Umowy.
10. **Wykonawca** przedstawi **Zamawiającemu** przed rozpoczęciem wykonywania przedmiotu Umowy, w formie oświadczenia adresy e-mail i telefony do osób odpowiedzialnych za usuwanie awarii dostarczanego systemu, w czasie trwania całego okresu gwarancyjnego.
11. **Wykonawca** w czasie wykonywania przedmiotu Umowy zobowiązany jest na żądanie **Zamawiającego** udzielić wyjaśnień dotyczących postępu i przebiegu prac.
12. **Wykonawca** przygotuje i przekaze **Zamawiającemu** oświadczenie o możliwości uzyskania kodów źródłowych.
13. **Wykonawca** zobowiązuje się do dołożenia wszelkich starań, aby dostarczony przez niego system funkcjonował bezawaryjnie i pozbawiony był wad fizycznych czy błędów programowych.

14. **Wykonawca** zapewnia, że dane związane z oprogramowaniem, kluczami licencyjnymi oraz wynikami działania systemu nie będą udostępniane osobom trzecim bez zgody **Zamawiającego**.
15. **Wykonawca** przekaze wraz z systemem wszelkie dokumenty licencyjne niezbędne do korzystania z oprogramowania stanowiącego przedmiot niniejszej **Umowy** oraz potwierdzające prawo do legalnego korzystania z przedmiotowego oprogramowania.
16. **Wykonawca** oświadcza niniejszym, iż korzystanie przez **Zamawiającego** z przedmiotu **Umowy** na warunkach w niej przewidzianych nie będzie naruszać praw autorskich, praw własności przemysłowej lub innych prawem chronionych dóbr osobistych lub majątkowych osób trzecich. W razie zgłoszenia przez osoby trzecie w związku z wykonywaniem przez **Zamawiającego** umowy jakichkolwiek roszczeń, **Wykonawca** bierze na siebie wyłączną odpowiedzialność z tytułu szkód majątkowych i niemajątkowych w mieniu i na osobie tych osób, a wynikłych z wykonania, z nienależytego wykonania lub z braku wykonania **Umowy** przez **Wykonawcę**.

§ 5

Wynagrodzenie Wykonawcy

1. Za wykonanie przedmiotu Umowy określonego w § 1 **Strony** ustalają wynagrodzenie umowne ogółem w następującej wysokości:
kwota netto zł (słownie złotych :, 00/100)
podatek VAT 23%, zł (słownie złotych:, 00/100)
kwota brutto zł (słownie złotych :, 00/100)
2. Określone w ust.1 wynagrodzenie obejmuje w szczególności wszelkie czynności podejmowane przez **Wykonawcę** niezbędne do prawidłowego wykonania przedmiotu Umowy.
3. Wynagrodzenie określone w ust.1 może ulec zmniejszeniu/zwiększeniu w przypadku zmniejszenia/zwiększenia zakresu rzeczowego określonego Umową. Z tytułu zmiany zakresu rzeczowego przedmiotu zamówienia i w konsekwencji zmiany wysokości wynagrodzenia **Wykonawcy** nie przysługują żadne roszczenia.
4. **Wykonawca** nie może przenieść na osoby trzecie swoich wierzytelności wynikających z Umowy bez uprzedniej pisemnej zgody **Zamawiającego**.

§ 6

Warunki płatności

1. Należność za wykonanie przedmiotu Umowy będzie płatna przez **Zamawiającego** na rachunek **Wykonawcy** zgłoszony do Naczelnika Urzędu Skarbowego, prowadzony w w terminie 30 dni od daty prawidłowego wystawienia i otrzymania przez **Zamawiającego** faktury VAT za wykonanie przedmiotu Umowy. Na fakturze powinien być umieszczony zapis "Mechanizm podzielonej płatności".
2. Podstawą do wystawienia faktury przez Wykonawcę jest podpisany przez obie Strony Protokół końcowy odbioru prac bez uwag i zastrzeżeń.
3. Za dzień dokonania zapłaty przyjmuje się dzień obciążenia rachunku bankowego **Zamawiającego**.

§ 7

Przedstawiciele stron

1. Osobami sprawującymi nadzór nad Umową i upoważnionymi do roboczych kontaktów (koordynatorzy) są:

a) ze strony **Zamawiającego**

Pantel:e-mail:

b) ze strony **Wykonawcy**

Pantel:e-mail:

2. Koordynatorzy są związani warunkami i terminami ustalonymi w Umowie.
3. Każda ze **Stron** zobowiązuje się zawiadomić na piśmie drugą **Stronę** o zmianie swojego koordynatora. Dla skutecznej zmiany koordynatora nie jest konieczne dokonanie zmiany Umowy.
4. **Strony** dopuszczają prowadzenie korespondencji pomiędzy osobami wymienionymi w ust. 1 w formie elektronicznej.

§ 8

Zintegrowany System Zarządzania

W związku z tym, że **Zamawiający** posiada Zintegrowany System Zarządzania, **Wykonawca** przyjmuje do wiadomości i zobowiązuje się do przestrzegania zasad Zintegrowanego Systemu Zarządzania wdrożonych według norm: PN-EN ISO 9001 : 2015-10, PN-EN ISO 14001 : 2015-09, PN - N 18001 : 2004 w zakresie współpracy z **Zamawiającym**.

§ 9

Odbiór przedmiotu Umowy

1. Po wykonaniu wszystkich prac, o których mowa w § 1 ust. 1 niniejszej Umowy, w szczególności przedstawienia raportu z przeglądu cyberzagrożeń przedsiębiorstwa, przeprowadzenia szkolenia dla pracowników **Zamawiającego** oraz po sprawdzeniu przez nich funkcjonalności przekazanych modułów, **Zamawiający** zweryfikuje wykonanie prac oraz sposób ich wykonania. Z czynności tej zostanie sporządzony Protokół końcowy odbioru prac, który będzie podstawą do otrzymania przez **Wykonawcę** wynagrodzenia umownego.
2. **Zamawiający** przystąpi do odbioru prac w terminie nie dłuższym niż 7 dni od momentu pisemnego zgłoszenia przez **Wykonawcę** gotowości prac do odbioru.
3. Jeżeli **Zamawiający** uzna, po wystąpieniu przez **Wykonawcę** z wnioskiem o dokonanie odbioru końcowego, że wykonanie przedmiotu Umowy zostało zakończone i nie będzie miał zastrzeżeń, wyznaczy datę odbioru końcowego w ciągu 7 dni od daty ich zgłoszenia przez **Wykonawcę**.
4. **Zamawiający** dokona odbioru prac zgłoszonych przez **Wykonawcę** pod warunkiem, że prace te zostały wykonane zgodnie z warunkami wykonania przedmiotu Umowy wskazanymi w §1, w szczególności z: SIWZ, Ofertą Wykonawcy, z przepisami prawa, zasadami wiedzy technicznej, warunkami technicznego wykonania i odbioru prac oraz po stwierdzeniu, że **Wykonawca** przekazał wszystkie wymagane dokumenty.
5. **Zamawiający** może wstrzymać się od dokonania odbioru zgłoszonych przez **Wykonawcę** prac w przypadku, gdy zakres zgłoszonych prac jest niezgodny lub nie odpowiada wymaganiom określonym w niniejszej Umowie. **Zamawiający** wyznaczy **Wykonawcy** termin do usunięcia wad przedmiotu odbioru. Jeżeli wady nie zostaną usunięte w terminie wskazanym przez **Zamawiającego** **Wykonawca** od chwili upływu tego terminu będzie pozostawał w zwłoce co do zakończenia prac i podlega karom umownym zgodnie z postanowieniami §12.
6. Jeżeli w toku czynności odbiorowych zostaną stwierdzone wady, to **Zamawiającemu** przysługują następujące uprawnienia:
 - a) jeżeli wady nadają się do usunięcia, może odmówić odbioru do czasu usunięcia wad,
 - b) jeżeli wady nie nadają się do usunięcia to :
 - jeżeli nie uniemożliwiają one użytkowania przedmiotu odbioru zgodnie z przeznaczeniem, **Zamawiający** może obniżyć odpowiednio wynagrodzenie,
 - jeżeli wady uniemożliwiają użytkowanie zgodnie z przeznaczeniem, **Zamawiający** może dostąpić od Umowy lub żądać wykonania przedmiotu Umowy po raz drugi.
7. **Strony** postanawiają, że z czynności odbioru będzie spisany *Protokół końcowy odbioru prac* zawierający wszelkie ustalenia dokonane w toku odbioru, jak też terminy wyznaczone na usunięcie stwierdzonych przy odbiorze wad.
8. Za datę zakończenia prac przyjmuje się datę odbioru przedmiotu Umowy przez **Zamawiającego**.

§ 10**Prace dodatkowe**

1. Jeżeli w trakcie wykonywania Umowy którakolwiek ze **Stron** stwierdzi konieczność wykonania prac dodatkowych lub zamiennych nie objętych zakresem Umowy, o którym mowa w §1 Umowy, zawiadomi o powyższym drugą **Stronę** Umowy.
2. Wykonanie dodatkowego zakresu prac możliwe będzie na podstawie zlecenia prac przez **Zamawiającego** (*Protokół prac dodatkowych/zamiennych* sporządzony przez obie **Strony**).
3. Wynagrodzenie za wykonane prace dodatkowe ustalone będzie odrębnymi negocjacjami **Stron**. **Wykonawca** zobowiązany jest wykonać to zamówienie według tych samych norm, standardów co zamówienie podstawowe.
4. Zapłata za wykonanie prac dodatkowych lub zamiennych, może nastąpić po podpisaniu przez **Strony** *Protokołu prac dodatkowych/zamiennych* określającego zakres i wartość prac oraz po podpisaniu stosownego Aneksu do Umowy.
5. Zapłata za wykonanie prac dodatkowych może nastąpić jedynie wówczas, gdy **Wykonawca**, przy dołożeniu należytej staranności nie mógł przewidzieć tych prac.
6. W przypadku wykonania prac, o których mowa w ust. 1 bez podpisania przez Strony stosownego *Protokołu prac dodatkowych/zamiennych* oraz Aneksu do Umowy **Wykonawcy** nie należy się dodatkowe wynagrodzenie.

§ 11**Gwarancja i rękojmia**

1. **Wykonawca** ponosi wobec **Zamawiającego** odpowiedzialność z tytułu rękojmi za wady przedmiotu Umowy przez okres (.....) **lat** od daty odbioru końcowego prac będących przedmiotem Umowy, na zasadach określonych w Kodeksie Cywilnym.
2. **Wykonawca** udziela **Zamawiającemu** na przedmiot niniejszej Umowy, gwarancji jakości na okres (.....) **lat**, licząc od daty odbioru końcowego prac będących przedmiotem Umowy.
3. W czasie trwania gwarancji **Wykonawca** zobowiąże się do świadczenia usług serwisowych Systemu polegających na wykonywaniu czynności skutkujących rozwiązaniem problemu oraz świadczenia konsultacji technicznych.
 - Czas odpowiedzi serwisu na zgłoszenie awarii powinien wynosić maksymalnie **8** godzin,
 - Czas przywrócenia działania sprawności sytemu do pracy ma wynosić maksymalnie **2** dni robocze,
 - Czas całkowitego rozwiązania problemu w wprowadzonym systemie to maksymalnie **7** dni roboczych.
4. Koszt serwisu w czasie trwania gwarancji spoczywa na **Wykonawcy**.
5. Wykonawca przedstawi **Zamawiającemu** w formie oświadczenia adresy e-mailowe, telefony do osób odpowiedzialnych za usuwanie awarii dostarczanego systemu w czasie trwania całego okresu gwarancyjnego
6. W przypadku, gdy **Wykonawca** nie przystępuje do usuwania wad lub usunie wady w sposób nienależyty, **Zamawiający**, poza uprawnieniami przysługującymi mu na podstawie Kodeksu Cywilnego i niniejszej Umowy, może powierzyć usunięcie wad podmiotowi trzeciemu na koszt i ryzyko **Wykonawcy** (wykonanie zastępcze), po uprzednim wezwaniu **Wykonawcy** i wyznaczeniu dodatkowego terminu nie krótszego niż 7 dni roboczych, bez utraty uprawnień wynikających z rękojmi i gwarancji.
7. Usunięcie wad następuje na koszt i ryzyko **Wykonawcy**.
8. Udzielona rękojmia i gwarancja nie naruszają prawa **Zamawiającego** do dochodzenia roszczeń o naprawienie szkody w pełnej wysokości na zasadach określonych w Kodeksie Cywilnym.
9. Bieg terminu gwarancji rozpoczyna się w dniu następnym po odbiorze końcowym robót objętych przedmiotem Umowy.
10. Gwarancja nie wyłącza, nie ogranicza, ani nie zawiesza uprawnień **Zamawiającego** wynikających z przepisów o rękojmi za wady.
11. W okresie gwarancji **Wykonawca** zobowiązuje się do usunięcia ujawnionych wad na własny koszt w terminie ustalonym z **Zamawiającym**.

12. Jeżeli **Wykonawca** dokonał usunięcia wady istotnej termin gwarancji biegnie na nowo od chwili usunięcia wady. W innych wypadkach termin gwarancji ulega przedłużeniu o czas, w którym **Zamawiający** nie mógł korzystać z przedmiotu Umowy.
13. Pomimo wygaśnięcia gwarancji lub rękojmi **Wykonawca** zobowiązany jest usunąć wady, które zostały zgłoszone przez **Zamawiającego** w okresie trwania gwarancji lub rękojmi.
14. **Wykonawca** zobowiązuje się w terminie obowiązywania rękojmi i gwarancji - to jest w terminie lat od dnia odbioru końcowego prac będących przedmiotem Umowy - usunąć wszystkie ujawnione wady dotyczące realizacji przedmiotu Umowy.

§ 12

Kary umowne

1. **Strony** ponoszą odpowiedzialność z tytułu niewykonania lub nienależytego wykonania Umowy na warunkach w niej określonych.
2. **Wykonawca** zapłaci **Zamawiającemu** następujące kary umowne:
 - a) w przypadku odstąpienia od Umowy z przyczyn niezależnych od **Zamawiającego** - 20 % wartości wynagrodzenia umownego brutto, o którym mowa w § 5 ust. 1 Umowy,
 - b) za każdy dzień zwłoki w zakończeniu prac będących przedmiotem niniejszej Umowy - 0,2 % wartości umownego wynagrodzenia brutto, o którym mowa w § 5 ust. 1 Umowy,
 - c) za nieterminowe usunięcie wad i usterek stwierdzonych przy odbiorze prac w wysokości 0,2 % wynagrodzenia umownego brutto, o którym mowa w § 5 ust. 1 Umowy, za każdy rozpoczęty dzień zwłoki liczony od dnia wyznaczonego na usunięcie wad.
 - d) za nieterminowe usunięcie wad i usterek, do usunięcia których **Wykonawca** jest zobowiązany z tytułu udzielonej gwarancji i rękojmi w szczególności w zakresie świadczenia usługi serwisowej, 0,2 % wartości wynagrodzenia umownego brutto, o którym mowa w § 5 ust. 1 Umowy, za każdy rozpoczęty dzień zwłoki w stosunku do terminu, w którym miało nastąpić usunięcie wady.
3. Odstąpienie od Umowy, którejkolwiek ze stron nie niweczy możliwości dochodzenia kar umownych.
4. **Strony** zastrzegają sobie prawo do odszkodowania uzupełniającego przekraczającego kary umowne do wysokości uzasadnionych rzeczywiście poniesionych szkód.
5. **Strony** dopuszczają możliwość zaniechania naliczania kar umownych na zasadach określonych w osobnym porozumieniu.
6. W razie obowiązku uiszczenia przez **Wykonawcę** kary umownej, jej wysokość może być potrącona przez **Zamawiającego** z wynagrodzenia należnego **Wykonawcy**, na co **Wykonawca** wyraża zgodę.

§ 13

Przetwarzanie danych osobowych

Zgodnie z art. 13 ust. 1–2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1) – dalej RODO - informujemy, że:

- 1) "Wodociągi Białostockie" Spółka z o.o. w Białymstoku, ul. Młynowa 52/1 jest administratorem danych osobowych.
- 2) Kontakt z Inspektorem Ochrony Danych, powołanym przez Przedsiębiorstwo: adres email: rodo@wobi.pl, iod@wobi.pl.
- 3) Pani/Pana dane osobowe przetwarzane będą:
 - na podstawie Art. 6 ust. 1 lit. b ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r potrzeb realizacji wniosku albo Umowy.
 - na podstawie Art. 6 ust. 1 lit. c ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 w celu świadczenia usług wynikających z Umowy Spółki oraz powszechnie obowiązujących przepisów prawa w tym w szczególności ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków (Dz. U. 2018. 1152 t.j.)

- na podstawie Art. 6 ust. 1 lit. f ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 w celu marketingu własnych produktów i usług a także dochodzenia roszczeń z tytułu prowadzonej działalności gospodarczej.
- 4) Pani/Pana dane osobowe będą przetwarzane przez okres wymagany przepisami prawa, chyba że niezbędny będzie dłuższy okres przetwarzania np. z uwagi na obowiązki archiwizacyjne, dochodzenie lub obronę roszczeń.
- 5) Odbiorcami Pani/Pana danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa oraz podmioty współpracujące w zakresie realizacji wniosku albo Umowy.
- 6) Pani/Panu przysługuje prawo do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do przenoszenia danych, prawo do cofnięcia zgody w dowolnym momencie.
- 7) Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa,
- 8) Podanie danych osobowych jest obligatoryjne w oparciu o przepisy prawa a w pozostałym zakresie jest dobrowolne.
- 9) Wykonawca zobowiązuje się poinformować osoby fizyczne nie podpisujące niniejszej umowy o treści niniejszych postanowień.

§ 14 Poufność

1. **Strony** zobowiązują się zachować w poufności wszelkie informacje uzyskane w wyniku zawarcia i/lub wykonywania postanowień niniejszej Umowy w szczególności o charakterze gospodarczym, handlowym, technicznym, technologicznym, finansowym, operacyjnym, prawnym, administracyjnym, organizacyjnym i innym, dotyczące którejkolwiek ze **Stron** niniejszej Umowy, niezależnie od formy ich przekazania i ich źródła, w których posiadanie **Strony** weszły w związku z zawarciem i/lub wykonywaniem Umowy, w tym w szczególności wszelkie wyniki i rezultaty prac wykonywanych na podstawie niniejszej Umowy oraz powstrzymywać się od używania informacji poufnych do celów innych niż te, dla których zostały one pierwotnie przekazane, jak również nie przekazywać żadnej informacji poufnej jakiegokolwiek osobie trzeciej (informacje poufne).
2. **Strony** gwarantują zachowanie poufności danych i zobowiązują się w szczególności do :
 - nie ujawniania w jakiegokolwiek formie informacji poufnych dotyczących wszystkich aspektów współpracy dotyczących realizacji Umowy jakiegokolwiek osobie trzeciej,
 - ochrony poufnych informacji uzyskanych w toku realizacji Umowy przy dochowaniu należytej staranności,
 - zwrócenia lub zniszczenia na pisemne żądanie dokumentów lub innych nośników informacji poufnych pochodzących od obu Stron, wraz z ich kopiami.
3. **Strony** zobowiązują się poinformować wszystkie osoby, które z uwagi na udział w realizacji Umowy będą miały styczność z informacjami poufnymi o obowiązku zachowania zasad poufności. **Strony** ponoszą odpowiedzialność za wszelkie naruszenia obowiązku poufności przez wskazane osoby jak za własne działanie.
4. Jeżeli w toku realizacji przedmiotu Umowy **Strony** uzyskały dostęp do informacji, które są wzajemnie poufne, zobowiązują się zachować pełną tajemnicę w tym zakresie i nie udostępniać tych informacji osobom trzecim ani wykorzystywać ich w sposób mogący szkodzić interesom drugiej **Strony**.
5. **Strony** zobowiązują się wykorzystywać uzyskane od drugiej **Strony** informacje tylko w celu wykonania swoich zobowiązań wynikających z niniejszej Umowy.
6. Informacje poufne mogą być ujawniane jedynie tym pracownikom lub współpracownikom **Stron** lub pracownikom przedsiębiorstw zależnych, kontrolowanych przez **Strony**, wobec których ujawnienie takie będzie uzasadnione i tylko w zakresie, w jakim odbiorca informacji musi mieć do nich dostęp dla realizacji postanowień niniejszej Umowy.
7. Strony podejmą wszelkie kroki w celu zapewnienia, że żadna z osób otrzymujących informacje poufne w rozumieniu Umowy nie ujawni ich ani ich źródła zarówno w całości, jak i w części, chyba, że otrzyma do tego wyraźne, pisemne upoważnienie od **Strony**, od której informacje poufne

- pochodzą. Upoważnienie takie określać będzie adresata informacji poufnych i zakres oraz cel, w jakich mają one być ujawnione.
8. **Stronom** nie wolno kopiować, powielać ani w jakikolwiek sposób rozpowszechniać informacji poufnych lub ich części, chyba, że jest to konieczne ze względu na realizację celów, o których mowa w ust.7 niniejszego paragrafu. Wszelkie kopie i reprodukcje stanowią własność **Zamawiającego**.
 9. Postanowień, o których mowa w ust. 6 - 10 nie stosuje się do informacji, które :
 - są opublikowane, oficjalnie podane do publicznej wiadomości, chyba, że do publikacji lub podania do publicznej wiadomości doszło z naruszeniem postanowień niniejszej Umowy lub przepisów dotyczących tajemnicy przedsiębiorstwa,
 - zostały zgodnie z prawem udostępnione przez osobę trzecią bez naruszania jakichkolwiek zobowiązań o ich nieujawnianiu w stosunku do **Stron** niniejszej Umowy,
 - zostały upublicznione na podstawie bezwzględnie obowiązujących przepisów prawa,
 - zostaną ujawnione przez jedną ze **Stron** za uprzednią zgodą drugiej **Strony**, wyrażoną zgodnie z postanowieniami ust.9 niniejszego paragrafu.
 10. Postanowienia dotyczące zachowania poufności obowiązują od dnia powzięcia informacji, o których mowa w ust. 6, w trakcie realizacji Umowy oraz w okresie po jej rozwiązaniu, wygaśnięciu, odstąpieniu przez jedną ze **Stron**.

§ 15

Odstąpienie od umowy

1. Jeżeli **Wykonawca** opóźnia się z rozpoczęciem lub zakończeniem realizacji przedmiotu Umowy tak dalece, że nie jest prawdopodobne, żeby zdołał go ukończyć w terminach określonych w § 2, **Zamawiający** może, bez wyznaczenia terminu dodatkowego, od Umowy odstąpić jeszcze przed upływem terminu wyznaczonego do wykonania przedmiotu Umowy.
2. Jeżeli **Wykonawca** realizuje przedmiot Umowy w sposób wadliwy albo sprzeczny z warunkami Umowy, **Zamawiający** może wezwać go do zmiany sposobu wykonania i wyznaczyć mu w tym celu odpowiedni termin. Po bezskutecznym upływie wyznaczonego terminu **Zamawiający** może od Umowy odstąpić bądź ją rozwiązać.
3. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy, **Zamawiający** może odstąpić od Umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach. W takim wypadku **Wykonawca** może żądać jedynie wynagrodzenia należnego mu z tytułu wykonanej części Umowy.
4. Odstąpienie od Umowy wskazane w ust. 1 i 2 uznaje się za odstąpienie od Umowy z przyczyn niezależnych of Zamawiającego.

§ 16

Klauzula antykorupcyjna

1. Wykonawca oświadcza, że w relacjach z Zamawiającym:
 - a. zobowiązuje się do przestrzegania powszechnie obowiązujących przepisów antykorupcyjnych,
 - b. nie podejmował jakichkolwiek działań, które miałyby na celu wpłynięcie na przebieg postępowania o udzielenie zamówienia lub wynik takiego postępowania oraz zawarcie Umowy w sposób sprzeczny z prawem lub dobrymi obyczajami,
 - c. nie będzie żądał, proponował, przyjmował oraz wręczał jakichkolwiek korzyści (zarówno osobistych jak i majątkowych) celem wywarcia korupcyjnego wpływu na decyzje, czy wykonywanie czynności służbowych przez osoby/podmioty zaangażowane w proces realizacji Umowy,
 - d. żadna część wynagrodzenia z tytułu realizacji Umowy nie będzie przeznaczona na pokrycie kosztów udzielania przez Wykonawcę korzyści majątkowych lub/i osobistych przez żadną ze Stron,
 - e. w dniu podpisania niniejszej Umowy nie pozostaje (zgodnie z jego najlepszą wiedzą) w konflikcie interesów mającym lub potencjalnie mogącym mieć wpływ na sposób

wykonywania obowiązków umownych, jak również nie są mu znane żadne inne okoliczności mogące wpłynąć na jego rzetelność, bezstronność i jakość wykonywanych prac lub usług.

§ 17 Zmiany w Umowie

1. **Zamawiający** przewiduje możliwość wprowadzenia, w wyniku zgodnego oświadczenia woli **Stron** Umowy, zmian postanowień zawartej Umowy w stosunku do treści oferty na podstawie, której dokonano wyboru Wykonawcy.
2. Zmiany niniejszej Umowy, o których mowa w ust 1. mogą być dokonywane jedynie w formie pisemnych aneksów podpisanych przez **Zamawiającego** i **Wykonawcę** pod rygorem nieważności.

§ 18 Inne postanowienia

1. **Zamawiający** nie dopuszcza możliwości wykonania przedmiotu Umowy przez podwykonawców.
2. W sprawach nieuregulowanych niniejszą Umową mają zastosowanie przepisy Kodeksu cywilnego.
3. **Strony** oświadczają, że ewentualne spory powstałe na tle realizacji niniejszej Umowy będą rozwiązywane polubownie, a w przypadku braku porozumienia rozstrzygane będą przez sąd właściwy miejscowo dla siedziby **Zamawiającego**.
4. Wszelka korespondencja między **Stronami** (w tym: powiadomienia, zawiadomienia, oświadczenia woli i wiedzy), z wyłączeniem bieżących kontaktów, o których mowa w § 7 Umowy, będzie kierowana na następujące adresy:
 - a) **Wykonawca** –, e-mail:
 - b) **Zamawiający** – Wodociągi Białostockie sp. z o.o. ul. Młynowa 52/1 15-404 Białystok, e-mail: sekretariat@wobi.pl
5. O każdej zmianie adresu **Strona** jest zobowiązana powiadomić niezwłocznie drugą **Stronę** na piśmie.
6. Niedopełnienie obowiązku określonego w ust. 5 skutkuje uznaniem za doręczoną korespondencji wysłanej na poprzednio wskazany adres.
7. Wszelkie oświadczenia woli **Strony**, wynikające z postanowień Umowy winny być dokonywane wyłącznie w formie pisemnej pod rygorem nieważności.
8. Integralną częścią Umowy są następujące dokumenty:
 - a) Załącznik nr 1 – Specyfikacja Istotnych Warunków Zamówienia w przetargu nieograniczonym na „Przeprowadzenie przeglądu cyberzagrożeń przedsiębiorstwa w oparciu o wdrożenie systemu typu GRC (Governance, Risk Management, Compliance - Ład Korporacyjny, Zarządzanie Ryzykiem, Zgodność)”,
 - b) Załącznik nr 2 – Umowa powierzenia przetwarzania danych osobowych,
 - c) Załącznik nr 3 – Oświadczenie Wykonawcy dotyczące możliwości pozyskania kodów źródłowych wdrażanego systemu,
 - d) Załącznik nr 4 - Oferta Wykonawcy.
9. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze **Stron**.

ZAMAWIAJĄCY

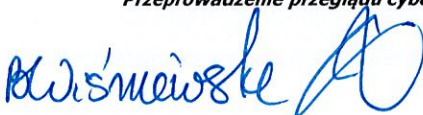
WYKONAWCA

.....

.....

.....

.....



Umowa powierzenia przetwarzania danych osobowych

zawarta w dniu2020 r., w Białymstoku pomiędzy:

Wodociągami Białostockimi Sp. z o.o. z siedzibą w Białymstoku przy ul. Młynowej 52/1, 15-950 Białystok, wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy w Białymstoku XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000024985, NIP: 5420200122, REGON: 050207647, z kapitałem zakładowym 165 540 000,00 zł zwaną dalej w treści umowy **Powierzającym**, reprezentowaną przez:

1)

2)

a

.....
.....
.....
.....

zwaną dalej **Przetwarzającym**, reprezentowaną przez:

1)

2)

zwani każda z osobna Stroną, a łącznie Stronami,

§1. Definicje

Ilekcóż poniższe pojęcia zostaną napisane w Umowie z dużej litery, Strony Umowy nadają im znaczenie wskazane w poniższych definicjach:

- 1) Umowa - oznacza niniejszą umowę wraz z załącznikami;
- 2) Umowa główna – oznacza umowę zawartą pomiędzy Stronami Nr **2 / NI / 2020** z dnia2020r., której przedmiotem jest Przeprowadzenie przeglądu cyberzagrożeń przedsiębiorstwa w oparciu o wdrożenie systemu typu GRC (Governance, Risk Management, Compliance - Ład Korporacyjny, Zarządzanie Ryzykiem, Zgodność) przez Przetwarzającego oraz sprawowanie opieki serwisowej i autorskiej nad przedmiotem umowy;

- 3) Dni robocze - oznaczają dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy, o których mowa w ustawie z dnia 18 stycznia 1951 roku o dniach wolnych od pracy (tekst jednolity: Dz. U. z 2015 r. poz. 90), przypadających w którykolwiek z tych dni (tj. od poniedziałku do piątku);
- 4) RODO - 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1).

W przypadku zastosowania w niniejszej Umowie pojęć zdefiniowanych w Umowie głównej pojęcia te będą rozumiane przez Strony niniejszej Umowy zgodnie z ich definicją określoną w Umowie głównej.

§2. Przedmiot przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą

1. Powierzający zgodnie z art. 28 ust. 3 RODO powierza Przetwarzającemu przetwarzanie danych osobowych określonych w Załączniku nr 1 do Umowy, których jest administratorem (w rozumieniu art. 4 pkt 7 RODO), a Przetwarzający (jako podmiot przetwarzający w rozumieniu art. 4 pkt 8 RODO) zobowiązuje się do przetwarzania tych danych osobowych zgodnie z niniejszą Umową. Pod pojęciem danych osobowych użytym w Umowie Strony rozumieją dane osobowe zdefiniowane w art. 4 pkt 1 RODO, których rodzaj i zakres został wskazany w niniejszej Umowie.
2. Powierzenie przetwarzania danych osobowych, o których mowa w ust. 1 następuje w celu realizacji Umowy głównej.
3. Powierzenie przetwarzania danych osobowych, o których mowa w ust. 1 następuje w zakresie określonym w Załączniku nr 1 do Umowy, w którym określony zostanie również rodzaj danych osobowych oraz kategorie osób, których dane dotyczą powierzone do przetwarzania Przetwarzającemu.
4. Przetwarzanie danych osobowych powierzonych Przetwarzającemu do przetwarzania będzie miało charakter stały, który wynika z Umowy głównej i określony jest rolą Przetwarzającego jako podmiotu świadczącego w sposób ciągły usługi sprawowania opieki serwisowej i autorskiej nad Systemem Aplikacyjnym.
5. Przetwarzanie odbywać się będzie w formie elektronicznej w systemach informatycznych lub formie papierowej poprzez wykonywanie wszystkich czynności (operacji na danych osobowych) uzasadnionych wykonywaniem lub realizacją Umowy głównej. Przetwarzający będzie w szczególności wykonywał następujące operacje dotyczące powierzonych danych osobowych: porządkowanie, adaptowanie lub modyfikowanie, przeglądanie, wykorzystywanie, dopasowywanie lub łączenie, pobieranie, organizowanie, ograniczanie, usuwanie lub niszczenie.
6. Dostęp do danych osobowych powierzonych do przetwarzania Przetwarzającemu na podstawie niniejszej Umowy odbywać się będzie za pośrednictwem szyfrowanego łącza VPN (ang. Virtual Private Network, Wirtualna Sieć Prywatna), aktywowanego w związku z realizacją Umowy głównej lub w innej szyfrowanej formie ustalonej pomiędzy Stronami. W przypadku danych osobowych przekazanych Przetwarzającemu na nośnikach danych zostaną one przekazane przez Powierzającego z zastosowaniem odpowiednich środków zabezpieczeń.

§3. Okres obowiązywania Umowy, czas trwania przetwarzania danych osobowych

1. Umowa zostaje zawarta na czas określony i obowiązuje począwszy od daty podpisania umowy głównej do końca obowiązywania okresu gwarancyjnego jaki został określony w Umowie głównej), z zastrzeżeniem ust. 2 i 3 poniżej.
2. W przypadku wcześniejszego rozwiązania lub wygaśnięcia (z dowolnej przyczyny) Umowy głównej (warunek) rozwiązaniu ulega również niniejsza Umowa, z zastrzeżeniem ust. 3.
3. Termin obowiązywania niniejszej Umowy zostaje wydłużony do dnia upływu terminu wskazanego w §4 ust. 12 in fine przewidzianego na wykonanie obowiązków w nim wskazanych.
4. Przetwarzanie danych osobowych powierzonych do przetwarzania Przetwarzającemu zgodnie z Umową odbywać się będzie w okresie obowiązywania niniejszej Umowy, a także w okresie gwarancyjnym i sprawowania opieki serwisowej.

§4. Oświadczenia i obowiązki Przetwarzającego

1. Przetwarzający zobowiązuje się wykonać zobowiązania określone w niniejszej Umowie z należytą starannością.
2. Przetwarzający będzie przetwarzał dane osobowe powierzone mu do przetwarzania zgodnie z niniejszą Umową wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Powierającego, przy czym Strony wskazują, iż Umowa główna i zgłoszenia serwisowe kierowane do Przetwarzającego na jej podstawie są i będą traktowane jako udokumentowane polecenia Powierającego. Za udokumentowane polecenia Powierającego będą uznawane również inne polecenia przekazywane przez Powierającego drogą elektroniczną na adres e-mail: lub na piśmie na adres wskazany w Umowie do doręczeń.
3. Przetwarzający oświadcza, że nie przekazuje danych osobowych powierzonych mu do przetwarzania zgodnie z niniejszą Umową do państwa trzeciego lub organizacji międzynarodowej.
4. Przetwarzający oświadcza, że podejmie po swojej stronie odpowiednie środki zabezpieczające dane osobowe powierzone mu do przetwarzania zgodnie z Umową, o których mowa w art. 32 RODO, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia tak, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
5. Przetwarzający oświadcza, że do wykonywania zobowiązań wynikających z postanowień Umowy będą dopuszczone wyłącznie osoby posiadające upoważnienia do przetwarzania danych osobowych nadane przez Przetwarzającego.
6. Przetwarzający prowadzić będzie ewidencję osób posiadających upoważnienia do przetwarzania danych osobowych na podstawie Umowy.
7. Przetwarzający zapewnia, że osoby, które zostały upoważnione do przetwarzania danych osobowych zgodnie z ust. 5 zostały zobowiązane do zachowania tajemnicy lub że podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy. Przetwarzający uzyskuje od tych osób udokumentowane oświadczenia zobowiązujące te osoby do zachowania tajemnicy, w tym także po wygaśnięciu zawartych z tymi osobami umów o pracę, umów cywilnoprawnych lub porozumień, na podstawie których osoby te świadczyły pracę/usługi na rzecz Przetwarzającego lub upewnia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy
8. Przetwarzający uwzględniając charakter przetwarzania oraz dostępne mu informacje będzie pomagał Powierającemu wywiązać się z obowiązków określonych w art. 32–36 RODO.

9. Przetwarzający biorąc pod uwagę charakter przetwarzania, w miarę możliwości będzie pomagał Powierzającemu poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO.
10. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Powierzającego, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.
11. W przypadku stwierdzenia przez Przetwarzającego naruszenia ochrony danych osobowych powierzonych mu do przetwarzania zgodnie z Umową, Przetwarzający zobowiązuje się bez zbędnej zwłoki zgłosić je Powierzającemu.
12. W terminie 30 Dni roboczych po zakończeniu świadczenia usług związanych z przetwarzaniem lub w przypadku wcześniejszego rozwiązania lub wygaśnięcia niniejszej Umowy (z dowolnej przyczyny) po jej rozwiązaniu lub wygaśnięciu, Przetwarzający zaleźnie od decyzji Powierzającego usunie lub zwróci mu wszelkie dane osobowe powierzone mu do przetwarzania zgodnie z Umową, oraz usunie wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych, z zastrzeżeniem zdania następnego. Zobowiązanie do usunięcia danych, o którym mowa w niniejszym ustępie nie dotyczy danych osobowych zgromadzonych/przetwarzanych za pomocą Systemu Aplikacyjnego w stosunku, do którego Przetwarzający świadczy usługi sprawowania opieki serwisowej i autorskiej, chyba, że Powierzający zdecyduje inaczej.

§5. Oświadczenia i obowiązki Powierzającego

1. Powierzający oświadcza, że jest administratorem (w rozumieniu art. 4 pkt 7 RODO) danych osobowych, o których mowa w §2 ust. 1 Umowy oraz, że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.
2. Powierzający zobowiązany jest współdziałać z Przetwarzającym w wykonaniu Umowy, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Powierzającego, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków określonych w niniejszej Umowie lub w innych udokumentowanych ustaleniach Stron.
3. Powierzający wysyłając - zgodnie z Umową główną – zgłoszenia serwisowe do Przetwarzającego zobowiązany jest do wdrożenia mechanizmów i procedur, które zapobiegać będą przesyłaniu danych osobowych w treści przedmiotowych zgłoszeń (tak aby nie zawierały one żadnych danych osobowych).
4. Powierzający zobowiązuje się przez czas obowiązywania Umowy oraz przez czas nieoznaczony po jej rozwiązaniu lub wygaśnięciu (z dowolnej przyczyny) do zachowania w poufności wszelkich informacji związanych z zabezpieczeniami technicznymi, organizacyjnymi lub innymi środkami zabezpieczającymi przetwarzanie danych osobowych stosowanymi po stronie Przetwarzającego w związku z realizacją Umowy i podjęcia działań aby osoby uzyskujące te informacje z jego strony zachowały je w tajemnicy także po wygaśnięciu zawartych z tymi osobami umów o pracę, umów cywilnoprawnych lub porozumień, na podstawie których osoby te świadczyły pracę/usługi na rzecz Powierzającego.
5. Powierzający w dniu zawarcia niniejszej Umowy przekaże Przetwarzającemu wszelkie informacje i warunki niezbędne do uzyskania bezpiecznego dostępu do danych osobowych powierzonych mu do przetwarzania na podstawie niniejszej Umowy lub też przekaże Przetwarzającemu te dane w sposób zabezpieczony przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem powszechnie obowiązujących

przepisów a także ich zmianą, utratą, uszkodzeniem lub zniszczeniem. W tym celu Powierzający stosuje odpowiednie środki techniczne i organizacyjne zapewniające stopień bezpieczeństwa odpowiadający poziomowi ryzyka naruszenia praw lub wolności osób fizycznych.

§6. Audyt

1. Przetwarzający udostępni Powierzającemu wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwi Powierzającemu lub audytorowi upoważnionemu przez Powierzającego przeprowadzanie audytów, w tym inspekcji. Przetwarzający będzie współpracował w zakresie realizacji audytów, w tym inspekcji.
2. O chęci skorzystania z uprawnień, o których mowa w ust. 1 Powierzający zobowiązany jest powiadomić Przetwarzającego na co najmniej 7 Dni roboczych przed planowanym audytem, w tym inspekcją.
3. Strony postanawiają, iż realizacja uprawnień, o których mowa w ust. 1 nie będzie mogła utrudniać bieżącej działalności Przetwarzającego.
4. Podczas realizacji uprawnień, o których mowa w ust. 1 Powierzający/audytor upoważniony przez Powierzającego zobowiązany będzie do poszanowania i stosowania się do polityki i regulaminów obowiązujących u Przetwarzającego w zakresie przetwarzania danych osobowych oraz do zachowania w tajemnicy przez okres wskazany przez Przetwarzającego wszelkich informacji stanowiących tajemnicę przedsiębiorstwa Przetwarzającego oraz innych informacji poufnych go dotyczących, w których posiadanie wejdzie Powierzający w związku z przeprowadzonym audytem, w tym inspekcją.
5. Przetwarzający zobowiązany jest również do umożliwienia przeprowadzenia przez właściwy organ administracji kontroli zgodności przetwarzania danych osobowych (powierzonych Przetwarzającemu do przetwarzania zgodnie z niniejszą Umową) z powszechnie obowiązującymi przepisami.

§7. Dalsze powierzenie przetwarzania danych osobowych

1. Powierzający wyraża niniejszym zgodę na dalsze powierzenie przetwarzania (podpowierzenie) przez Przetwarzającego danych osobowych (o których mowa w §2 ust. 1 Umowy) następującym innym podmiotom przetwarzającym:
 - a. Podmiot
 - b. Podmiot
 - c. Podmiot
2. Powierzający dopuszcza możliwość dalszego powierzenia przetwarzania (podpowierzenia) przez Przetwarzającego danych osobowych (o których mowa w §2 ust. 1 Umowy) innym podmiotom przetwarzającym, przy czym warunkiem dalszego powierzenia przetwarzania (podpowierzenia) jest:
 - 1) uprzednie poinformowanie Powierzającego przez Przetwarzającego o zamiarze dalszego powierzenia przetwarzania danych osobowych innym podmiotom przetwarzającym, (potencjalnym dalszym przetwarzającym/podprzetwarzającym) w zakresie konkretnych czynności przetwarzania lub dokonaniu zmiany w zakresie podmiotu będącego już dalszym przetwarzającym/podprzetwarzającym,
 - 2) brak zgłoszenia przez Powierzającego sprzeciwu dla zamierzonego dalszego powierzenia przetwarzania danych osobowych (podpowierzenia) w terminie 7 Dni roboczych licząc od dnia doręczenia Powierzającemu informacji, o której mowa w pkt 1 powyżej.

3. W przypadku uprzedniego poinformowania Powierzającego zgodnie z ust. 2 pkt 1 oraz niewyrażeniu sprzeciwu wobec dalszego powierzenia przetwarzania (podpowierzenia) w terminie wskazanym w ust. 2 pkt 2 przez Powierzającego, Przetwarzający uprawniony będzie do dokonania dalszego powierzenia przetwarzania (w zakresie konkretnych czynności przetwarzania) danych osobowych, o których mowa w §2 ust. 1 Umowy.
4. Dokonując dalszego powierzenia przetwarzania (podpowierzenia) w zakresie konkretnych czynności przetwarzania, Przetwarzający ma obowiązek zobowiązać dalszego przetwarzającego do realizacji wszystkich obowiązków Przetwarzającego wynikających z niniejszej Umowy, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO, z wyjątkiem tych, które nie mają zastosowania ze względu na naturę konkretnego dalszego powierzenia.
5. Przetwarzający będzie przestrzegał warunków korzystania z usług innego podmiotu przetwarzającego (dalszego przetwarzającego/podprzetwarzającego), o których mowa w art. 28 ust. 2 i 4 RODO.

§8. Rozwiązanie Umowy

Powierzający jest uprawniony do wypowiedzenia niniejszej Umowy ze skutkiem natychmiastowym (tj. bez okresu wypowiedzenia), gdy Przetwarzający:

- 1) pomimo uprzedniego, pisemnego wezwania go do usunięcia uchybień stwierdzonych podczas audytów, w tym inspekcji przeprowadzonych zgodnie z §6 Umowy nie usunie ich w wyznaczonym terminie, nie krótszym niż 14 Dni roboczych licząc od dnia doręczenia mu wezwania,
- 2) przetwarza dane osobowe w sposób niezgodny z Umową, pomimo uprzedniego, pisemnego wezwania go do zaprzestania niezgodnego z Umową przetwarzania danych w wyznaczonym terminie, nie krótszym niż 7 Dni roboczych licząc od dnia doręczenia mu wezwania,
- 3) powierzył przetwarzanie danych osobowych innemu podmiotowi bez uprzedniej zgody Powierzającego lub zachowania warunków dalszego powierzenia przetwarzania (podpowierzenia) określonych w §7 ust. 2 Umowy.

§9. Odpowiedzialność Przetwarzającego

1. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Powierzającego o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Przetwarzającego danych osobowych na podstawie niniejszej Umowy, o jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania przez Przetwarzającego tych danych osobowych, w szczególności prowadzonych przez administracyjny organ nadzoru, chyba, że poinformowanie Powierzającego będzie zabronione na podstawie obowiązujących przepisów prawa lub decyzji sądu lub administracyjnego organu nadzoru. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych Przetwarzającemu przez Powierzającego.
2. Przetwarzający ponosi względem Powierzającego odpowiedzialność odszkodowawczą z tytułu niewykonania lub nienależytego wykonania Umowy, w tym z tytułu niezgodnego z Umową przetwarzania danych osobowych.
3. Powierzający uprawniony jest do występowania do Przetwarzającego z ewentualnymi roszczeniami regresowymi Powierzającego względem Przetwarzającego w sytuacji, gdy

Przetwarzający okaże się odpowiedzialny/współodpowiedzialny za szkodę, którą poniosła osoba, której dane dotyczą w wyniku naruszenia RODO. Powierzający zobowiązany jest każdorazowo do poinformowania Przetwarzającego o każdym zdarzeniu, które mogłoby stanowić podstawę zgłoszenia przez Powierzającego roszczeń regresowych, o których mowa w zdaniu poprzednim w przypadku, gdy okoliczności zdarzenia wskazują na odpowiedzialność/współodpowiedzialność Przetwarzającego w powstaniu szkody oraz umożliwi Przetwarzającemu odniesienie się i wskazanie okoliczności, które wyłączają obowiązek naprawienia ewentualnej szkody przez Przetwarzającego jako podmiotu przetwarzającego.

§10. Postanowienia końcowe

1. Powierzający oświadcza, że funkcję ~~administratora bezpieczeństwa informacji~~/inspektora ochrony danych* (niepotrzebne skreślić) pełni u niego: **Rafał Nalewajko**, adres do korespondencji: **Formica Szerszenowicz s.j., ul. Gruntowa 9/1 lok.102**, tel.:**668 028 173**..... adres e-mail:**iod@wobi.pl**.....
2. Przetwarzający oświadcza, że funkcję inspektora ochrony danych pełni u niego: adres do korespondencji....., adres e-mail:
3. Zmiana danych osób wymienionych w ust. 1 i 2 nie stanowi zmiany Umowy. Zmiana taka następuje poprzez pisemne zawiadomienie drugiej Strony o zmianie.
4. Strony wskazują następujące adresy dla doręczeń:

Powierzający:

Przetwarzający:

Wodociągi Białostockie Sp. z o.o.
ul. Młynowa 52/1
15-001 Białystok

tel. (85) 74 58 100

tel.

5. Strony zobowiązują się do niezwłocznego informowania o wszelkich zmianach adresów do doręczeń pod rygorem uznania doręczenia pod ostatni wskazany adres do doręczeń za skuteczne. Zmiana adresu do doręczeń nie stanowi zmiany Umowy. Zmiana taka następuje poprzez pisemne zawiadomienie drugiej Strony o zmianie.
6. Mając na uwadze, iż niniejsza Umowa zawarta została w związku i w celu realizacji Umowy głównej Przetwarzający potwierdza, iż kalkulacja wynagrodzenia należnego Przetwarzającemu na podstawie Umowy głównej została dokonana przy uwzględnieniu zobowiązań Przetwarzającego wynikających z niniejszej Umowy i zobowiązania określone w niniejszej Umowie zostaną wykonane przez Przetwarzającego w ramach wynagrodzenia określonego w Umowie głównej.

7. Strony będą dążyć do polubownego rozstrzygnięcia wszelkich sporów, jakie mogą wyniknąć w związku z interpretacją lub wykonywaniem Umowy (postanowienie to nie stanowi zapisu na sąd polubowny).
8. Jeżeli działanie podjęte w myśl ust. 7 nie przyniosą rezultatu zadowolającego obie Strony, sądem właściwym do rozstrzygnięcia wszelkich sporów wynikających z niniejszej Umowy jest właściwy sąd powszechny dla siedziby Powierającego.
9. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności, z zastrzeżeniem wyjątków przewidzianych w Umowie. Oświadczenie o wypowiedzeniu/rozwiązaniu niniejszej Umowy lub odstąpieniu od Umowy również wymaga formy pisemnej pod rygorem nieważności.
10. Integralną częścią Umowy są załączniki wymienione w treści niniejszej Umowy.
11. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Załączniki:

- 1) *Załącznik nr 1 do Umowy – Zakres, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą powierzone do przetwarzania Przetwarzającemu.*

Powierający

Przetwarzający

Podpis osoby lub osób upoważnionej
(-ych) do reprezentacji

Podpis osoby lub osób upoważnionej
(-ych) do reprezentacji

Zakres, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą powierzone do przetwarzania Przetwarzającemu.

Rodzaj danych osobowych: dane zwykłe

W systemie pocztowym Groupwise:

Kategoria danych	Postać (Zakres)
Dane użytkowników usług katalogowych eDirectory / AD	<ol style="list-style-type: none"> 1. nazwisko, 2. pierwsze imię, 3. drugie imię, 4. adres e-mail, 5. nr telefonu, 6. komórka, 7. miejsce pracy,
Dane kontrahentów (Podmiotów) korespondujących z Powierzającym:	<ol style="list-style-type: none"> 1. Imię 2. Nazwisko 3. Imię Ojca 4. Imię Matki 5. Seria, nr i miejsce wydania dowodu osobistego 6. Pesel 7. Dane dotyczące działalności gospodarczej 8. Adres 9. Adres korespondencyjny 10. Telefon 11. Adres email 12. Nr konta bankowego 13. Źródło danych 14. Wyrażone zgody / sprzeciw w obec przetwarzania w celach marketingowych 15. Informacje dodatkowe zapisane w postaci niestrukturalnej typu: Komentarze, Uwagi, Notatki 16. Umowy związane z Płatnikiem 17. Faktury 18. Reklamacje 19. Rozliczenia 20. Urządzenia pomiarowe 21. Punkty adresowe 22. Zgody na polecenie zapłaty

Kategoria danych	Postać (Zakres)
	23. Zgody na e-wysyłkę
	24. Saldo finansowe

Rodzaj danych osobowych: szczególna kategoria danych osobowych

System nie wspiera przetwarzania szczególnych kategorii danych osobowych i nie zawiera dedykowanych zbiorów danych do przechowywania takich informacji.

Rodzaj danych osobowych: dane osób małoletnich

System nie wspiera przetwarzania szczególnych kategorii danych osobowych i nie zawiera dedykowanych zbiorów danych do przechowywania takich informacji.

Rodzaj danych osobowych: wyroki skazujące i naruszenia prawa

System nie wspiera przetwarzania danych osobowych w zakresie wyroków skazujących i naruszeń prawa i nie zawiera dedykowanych zbiorów danych do przechowywania takich informacji.

Blisniewske 