WODOCIĄGI BIAŁOSTOCKIE

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. 27.10.2021 r.

OGŁOSZENIE / SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA W PRZETARGU NIEOGRANICZONYM NA

Wdrożenie zabezpieczeń serwerowego środowiska teleinformatycznego.

Nr ref. sprawy: NI–I–9/2021

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 „Wdrożenie zabezpieczeń serwerowego środowiska teleinformatycznego”.**

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 wywieszone na tablicy ogłoszeń w siedzibie Zamawiającego, w Białymstoku przy ul. Młynowej 52/1.

I. OPIS PRZEDMIOTU ZAMÓWIENIA

TABELA NR 1 – opis minimalnych wymagań dla wdrożenia zabezpieczeń serwerowego środowiska teleinformatycznego.

WYMAGANIA OGÓLNE:
1. **Rozwiązanie musi być dostarczone w formie SaaS,** gdzie wszystkie komponenty centralne, takie jak centralny serwer zarządzający i jego bazy

danych, hostowane są w chmurze i dostarczone przez producenta oferowanego rozwiązania jako usługa. Producent oferowanego rozwiązania jest odpowiedzialny za bezpieczeństwo, niezawodność, skalowalność oraz aktualizacje wszystkich elementów centralnych dostarczanych jako usługa typu SaaS, a także nowe wersje dostarczanego produktu dostępne w ramach aktualizacji usługi.
2. **Licencjonowanie** oprogramowania musi być oparte na liczbie końcowych, objętych ochroną serwerów fizycznych oraz wirtualnych.
WYMAGANIA FUNKCJONALNE:
1. **Pełna administracja konfiguracją oprogramowania zabezpieczającego oraz monitorowanie środowiska** serwerów fizycznych i wirtualnych powinna odbywać się za pomocą jednej konsoli administracyjnej dostępnej z poziomu przeglądarki internetowej.
2. **Oprogramowanie zabezpieczające musi integrować się z systemem klasy EDR,** który będzie wykonywał zaawansowaną korelację zdarzeń przesyłanych przez system zabezpieczający, oraz inne systemy co najmniej tego samego producenta w celu wykonywania zaawansowanych korelacji, wykrywania ataków oraz aktywności potencjalnie niebezpiecznych.
3. **System klasy EDR powinien być również dostarczany w formie SaaS**, gdzie wszystkie komponenty systemu EDR hostowane są w chmurze i dostarczone przez producenta oferowanego rozwiązania jako usługa.
4. **System klasy EDR powinien być dostarczony razem z systemem zabezpieczeń serwerów wirtualnych i fizycznych.**
WYMAGANIA DOTYCZĄCE ZARZĄDZANIA INFRASTRUKTURĄ SYSTEMU ZABEZPIECZAJĄCEGO:
1. Rozwiązanie musi pozwalać na ochronę serwerów uruchomionych w lokalnym centrum przetwarzania danych zamawiającego **(on-prem), które funkcjonuje w oparciu o rozwiązanie VMware** lub serwery fizyczne.
2. Oprogramowanie zabezpieczające musi umożliwiać agentową ochronę maszyn fizycznych i wirtualnych.
3. Bieżące, automatyczne identyfikowanie i wyświetlanie **aktualnej listy maszyn wirtualnych** w konsoli administracyjnej.
4. Integracja ze środowiskami **Microsoft Active Directory, VMware vCenter** umożliwiająca odzwierciedlanie aktualnej listy maszyn wirtualnych uruchomionych w wymienionych środowiskach.
5. Oprogramowanie zabezpieczające musi być dostarczone z aktywnymi licencjami na opisane moduły funkcjonalne **na okres 3 lat**.
6. Oprogramowanie zabezpieczające musi zapewniać **bezpieczeństwo zarówno serwerów wirtualnych jak i maszyn fizycznych.**
7. Oprogramowanie zabezpieczające musi posiadać funkcjonalność określenia **harmonogramu lub częstotliwości pobierania aktualizacji bezpieczeństwa** od producenta oprogramowania;.

8. Oprogramowanie zabezpieczające musi posiadać funkcjonalność **zarządzania zdarzeniami i raportowanie – natychmiastowe alarmowanie** o aktywności niebezpiecznego kodu na chronionym serwerze.
9. Oprogramowanie zabezpieczające musi **umożliwiać nanoszenie zmian w profilach bezpieczeństwa w czasie rzeczywistym bez potrzeby restartu** systemu i chronionych obiektów.
10. Oprogramowanie zabezpieczające musi posiadać funkcjonalność zapewniającą **dostęp do konsoli z kilku stacji roboczych jednocześnie**.
11. Oprogramowanie zabezpieczające musi posiadać **wsparcie dla dostępu do konsoli z przeglądarek Microsoft Internet Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox bez stosowania dodatkowych komponentów lub rozszerzeń**;
12. Oprogramowanie zabezpieczające musi umożliwiać **personalizację widoku panelu głównego konsoli**;
13. Oprogramowanie zabezpieczające musi umożliwiać **ochronę następujących dystrybucji systemu operacyjnego Linux**: RedHat Enterprise Linux, CentOS, Oracle Linux, SUSE Linux, Ubuntu, Debian, Cloud Linux, Solaris, AIX, w różnych wersjach zainstalowanych u Zamawiającego;
14. Oprogramowanie antywirusowe musi umożliwiać **ochronę następujących dystrybucji systemu operacyjnego Windows**: Windows 2008, Windows 2008 R2, Windows 2012, Windows 2012 R2 Core, Windows 2016, Windows 2019
15. Funkcjonalność tworzenia **kont dla administratorów o różnych stopniach uprawnień** w odniesieniu do różnych chronionych maszyn wirtualnych lub ich grup z dokładnością do pojedynczej polityki lub serwera;
16. Oprogramowanie zabezpieczające musi mieć funkcjonalność **tworzenia ról administratorów i przydzielania im uprawnień, co najmniej w zakresie zarządzania**: • Serwerami lub grupami serwerów; • Politykami lub grupami polityk; • Poszczególnymi funkcjonalnościami oferowanego systemu;
17. **Zarządzanie rolami w systemie musi pozwalać na zdefiniowanie** uprawnień dających możliwość administrowania wyłącznie jednym chronionym obiektem oraz pojedynczymi funkcjonalnościami systemu bez możliwości zmiany nadrzędnego profilu bezpieczeństwa;
18. Oprogramowanie zabezpieczające musi mieć funkcjonalność **tworzenia logicznych grup serwerów w celu zarządzania tymi grupami** oraz wymuszania stosowania określonych dla grup zasad bezpieczeństwa, ustanawianych dla każdej z grypy indywidulanie;
19. Oprogramowanie antywirusowe musi mieć funkcjonalność **tworzenia drzewa polityk zależnych**, w którym polityki pochodne dziedziczą ustawienia od polityk na wyższym poziomie. Administratorzy posiadający uprawnienia jedynie do polityk pochodnych nie mogą mieć możliwości wprowadzania zmian do ustawień dziedziczonych.

WYMAGANIA DOTYCZĄCE FUNKCJONALNOŚCI W ZAKRESIE ANTYMALWARE I WEB REPUTATION
1. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność ciągłego, bieżącego i automatycznego wykrywania zagrożeń co najmniej typu**: „spyware", „greyware", „adware", „keylogger", „dialer", „trojan", „malware";
2. Oprogramowanie zabezpieczające musi posiadać efektywną **ochronę przed zagrożeniami typu** „ransomware";
3. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność określenia obszarów skanowania, typów skanowanych plików, momentu ich skanowania** (otwarcie i/lub modyfikacja) oraz na wykluczenie ze skanowania określonych obszarów dla skanowania w czasie rzeczywistym, ręcznego skanowania oraz skanowania określonego w harmonogramie;
4. Oprogramowanie zabezpieczające musi posiadać funkcjonalność **predefiniowania reakcji** w przypadku wykrycia wirusa, w tym co najmniej: czyszczenie, usunięcie, kwarantanna, oraz natychmiastowego automatycznego wykonywania tej reakcji, a także raportowania o zaistniałym zdarzeniu.
5. Oprogramowanie zabezpieczające musi zapewniać **określenie harmonogramu skanowania** (obiekty i grupy) oraz wymuszenia skanowania w danej chwili;
6. Oprogramowanie zabezpieczające musi stosować mechanizm **skanowania nowych bądź zmienionych plików** w celu skrócenia czasu skanowania oraz zwiększenia wydajności skanowania;
7. Oprogramowanie zabezpieczające musi posiadać funkcjonalność zdefiniowania **harmonogramu lub częstotliwości pobierania aktualizacji bazy wirusów, wszelkich poprawek oprogramowania** oraz umożliwiać określenie centralnego punktu dystrybucji uaktualnień i poprawek oprogramowania w infrastrukturze zamawiającego;
8. Oprogramowanie zabezpieczające musi posiadać funkcjonalność **predefiniowania reakcji w przypadku wykrycia wirusa**, w tym co najmniej: czyszczenie, usunięcie, kwarantanna.
9. Oprogramowanie zabezpieczające **nie może wymagać restartu** chronionych komputerów i serwerów **po dokonaniu aktualizacji** mechanizmów skanujących i definicji wirusów;
10. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność ciągłego, bieżącego i automatycznego blokowania połączeń** do adresów URL określonych przez producenta systemu, jako niebezpieczne, również w przypadku, gdy połączenia są nawiązywane przez procesy działające na chronionych serwerach, oraz bieżącego aktualizowania listy tych adresów;
11. Oprogramowanie zabezpieczające musi mieć funkcjonalność definiowania **statycznych list adresów URL**, do których połączenia są ciągle, na bieżąco i automatycznie blokowane;
12. Oprogramowanie zabezpieczające musi zapewniać **ochronę maszyn znajdujących się w strefie DMZ** (ang. demilitarized zone);

13. Oprogramowanie zabezpieczające musi mieć **funkcjonalność generowania i wysyłania e-mailem na zdefiniowany adres/adresy raportów** w wybranym formacie (co najmniej .pdf);
14. Oprogramowanie zabezpieczające musi posiadać możliwość integracji z systemami klasy **SIEM** po protokole **SYSlog** lub dedykowanej integracji z tym systemem.
15. **Serwer zarządzający oprogramowania zabezpieczającego powinien posiadać API** pozwalające na jego integrację z zewnętrznymi systemami zarządzającymi firm trzecich. Dokumentacja API zapewniająca integrację z zewnętrznymi systemami zarządzającymi firm trzecich musi być powszechnie dostępna;
16. **Narzędzie powinno dostarczać informacje o stanie bezpieczeństwa serwerów, w postaci logów, wysyłanych bezpośrednio do serwera Syslog**, które posiadany przez Zamawiającego system SecureVisio (ESECURE SP. Z O.O., ul. Hoffmanowej 19, PL-35016 Rzeszów) będzie w stanie zidentyfikować oraz wykorzystać w korelacjach dotyczących Reguł Bezpieczeństwa.
17. **Logi do systemu SecureVisio powinny być dostarczane w przypadku identyfikacji działań niepożądanych na serwerach,** umożliwiając również ich późniejszą analizę w systemie SecureVisio, w przypadku wystąpienia Incydentu.
WYMAGANIA DOTYCZĄCE FUNKCJONALNOŚCI W ZAKRESIE MONITOROWANIA INTEGRALNOŚCI I INSPEKCJI LOGÓW ORAZ KONTROLI APLIKACJI
1. Oprogramowanie zabezpieczające musi pozwalać na **monitorowanie pod kątem integralności wskazanych** plików, katalogów, serwisów, wpisów w rejestrach, listy uruchomionych procesów oraz otwartych portów i informowanie o wprowadzanych zmianach.
2. **Informacja o wprowadzonych zmianach musi zawierać, co najmniej** nazwę pliku lub wpisu w rejestrze, w którym została wprowadzona zmiana, datę i czas wprowadzenia zmiany, nazwę serwera, na którym została wprowadzona zmiana, oraz nazwę reguły, która została wykorzystana.
3. Oprogramowanie zabezpieczające musi umożliwiać **monitorowanie pod kątem integralności otwartych na objętym ochroną serwerze portów** – zamknięcie lub otwarcie nowego portu powinno być traktowane jako zmiana integralności i powinno generować zdarzenie bezpieczeństwa.
4. Oprogramowanie zabezpieczające musi umożliwiać **monitorowanie pod kątem integralności listy uruchomionych na objętym ochroną serwerze procesów** – zatrzymanie lub uruchomienie procesu powinno być traktowane jako zmiana integralności i powinno generować zdarzenie bezpieczeństwa.
5. **Oprogramowanie zabezpieczające musi posiadać predefiniowany zestaw reguł dostarczonych przez producenta oprogramowania** określających wskazane do monitorowania pliki, wpisy w rejestrach oraz monitorowane serwisy, w zależności od chronionego systemu lub aplikacji.

6. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność ręcznego definiowania reguł** dotyczących monitorowanych plików oraz wpisów w rejestrach;
7. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność definiowania wykluczeń** plików znajdujących się w monitorowanym katalogu;
8. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność analizy logów** pochodzących ze wskazanych systemów oraz aplikacji;
9. Oprogramowanie zabezpieczające musi **posiadać reguły dostarczone przez producenta określające wskazane do zbierania i analizy logi**, w zależności od chronionego systemu lub aplikacji;
10. Oprogramowanie zabezpieczające musi posiadać funkcjonalność r**ęcznego definiowania przez administratora zbieranych i analizowanych logów**;
11. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność dokonywania analizy logów co najmniej w formatach**: syslog, snort, apache, squid, iis, nmapg, mysql, postgresql, eventlog;
12. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność analizowania nieustandaryzowanych logów generowanych przez aplikacje i systemy**, w szczególności logów w postaci pojedynczej linijki tekstu;
13. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność definiowania poziomu krytyczności każdej z reguł logów**;
14. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność tworzenia polityk stanowiących zbiór reguł dostarczonych przez producenta** oraz zdefiniowanych przez administratora;
15. Oprogramowanie zabezpieczające musi posiadać **mechanizm kontroli aplikacji uniemożliwiający na instalowanie jakichkolwiek niezatwierdzonych do działania w środowisku aplikacji**. Oprogramowanie antywirusowe musi posiadać możliwość otwierania tzw. „okien czasowych”, w których zespoły mogą wprowadzać zmiany do konfiguracji aplikacji na serwerach;
WYMAGANIA DOTYCZĄCE FUNKCJONALNOŚCI W ZAKRESIE ZAPORY OGNIOWEJ (FIREWALL) ORAZ OCHRONY PRZED ATAKAMI SIECIOWYMI (INTRUSION PREVENTION)
1. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność ciągłej, bieżącej i automatycznej kontroli oraz blokowania skierowanych na serwer ataków w warstwie sieciowej**.
2. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność ciągłego, bieżącego i automatycznego wykrywania ataków typu SQL injection oraz cross-site-scripting** wraz z możliwością ustanowienia progów alarmu jak również dodawania i edytowania nowych ciągów danych;
3. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność przełączania pomiędzy trybem blokowania ruchu i trybem detekcji zdarzeń** w sposób globalny dla wszystkich reguł;

4. Oprogramowanie zabezpieczające musi **posiadać moduł zapewniający blokowanie transmisji na podstawie zdefiniowanej charakterystyki ruchu poprzez sygnatury oraz zdefiniowane ciągi znaków** (pattern'u).
5. Oprogramowanie zabezpieczające musi **posiadać możliwość automatycznego uruchamiania dla każdego z chronionych serwerów oddzielnie tzw. wirtualnych poprawek**, pozwalających na ochronę przed atakami wykorzystującymi podatności systemów operacyjnych i aplikacji do czasu zainstalowania standardowych poprawek producenta i restartu systemów;
6. Oprogramowanie zabezpieczające musi posiadać funkcjonalność **ochrony podatności wykrytych na serwerze Windows Server 2008 / 2008 R2 oraz nowszych. System musi posiadać** funkcjonalność **ochrony podatności wykrytych na serwerach Linux**
7. Oprogramowanie zabezpieczające musi posiadać **dwukierunkowy stanowy firewall** (stateful firewall) zapewniający izolację interfejsów bez konieczności restartów chronionych serwerów.
8. Oprogramowanie zabezpieczające powinno działać w protokole IPv4 jak i IPv6.
9. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność ciągłej, bieżącej i automatycznej kontroli połączeń wychodzących i przychodzących** w komunikacji sieciowej z możliwością kontroli **niestandardowych portów TCP** (funkcjonalność definiowania na podstawie numeru protokołu oraz numeru typu ramki);
10. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność przełączenia trybu działania reguł firewall z trybu blokowania ruchu w tryb detekcji zdarzeń**;
11. Oprogramowanie zabezpieczające musi **zapewniać analizę ruchu sieciowego pod kątem występowania anomalii**, w szczególności: zdeformowanych pakietów, brakujących flag;
12. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność definiowania trybu pracy „Tap"** (analiza kopii pakietu przychodzącego bez możliwości stosowania zasad ochrony - na potrzeby zapisu zdarzeń) **oraz „Inline"** (analiza pakietu przychodzącego wraz z zastosowaniem zasad ochrony) dla każdego chronionego obiektu i polityki bezpieczeństwa;
13. Oprogramowanie antywirusowe musi posiadać **możliwość definiowania polityk firewall oraz IPS dla każdego serwera wirtualnego** oddzielnie działających zarówno na ruchu pomiędzy środowiskiem VMware i zewnętrznym środowiskiem, jak i na ruchu pomiędzy maszynami wirtualnymi;
14. Oprogramowanie antywirusowe musi posiadać **funkcjonalność inspekcji HTTPS** bez konieczności instalacji dodatkowego oprogramowania.
WYMAGANIA DOTYCZĄCE FUNKCJONALNOŚCI SYSTEMU EDR
1. Oferowany system klasy **EDR musi posiadać możliwość zbierania danych z serwerów** w tym co najmniej: i. Procesy, w tym modyfikacja ii. Pliki

iii. Połączenia sieciowe
iv. Zapytania DNS
v. Rejestry
vi. Konta i użytkownicy
vii. Zdarzenia Internetowe (obsługa URL)
viii. Windows hooks
ix. detekcje

2. Dane zbierane z poszczególnych warstw mają być normalizowane i korelowane między sobą.
3. W wyniku korelacji system ma tworzyć incydenty o wysokim poziomie pewności (niski poziom false-positive).
4. **Dane mają być mapowane na matrycę TTP** (techniques, takctiques, procedures), z uwzględnieniem matrycy **MITRE ATT&CK**
5. **Zarządzanie:**
   - System ma posiadać mechanizm pozwalający na proste i intuicyjne uruchamianie sensorów na poszczególnych elementach środowiska
   - System ma pokazywać status sensora na poszczególnych zasobach, w tym pokazywać z jakiej przyczyny sensor nie może zostać uruchomiony
   - Mechanizm tworzenie kont w systemie powinien pozwalać na zdefiniowanie dostępu do poszczególnych funkcji systemu (np. dostęp tylko do dashboard lub dostęp do listy alertów)
6. **Raportowanie:**
   - System musi pozwalać na przedstawianie danych bezpieczeństwa w różnych perspektywach:
     i. Alerty,
     ii. Użytkownicy
     iii. Detekcje
     iv. Zdarzenia w matrycy MITRE ATT&CK
   - System ma pozwalać na wysyłanie notyfikacji do wybranego administratora odnośnie:
     i. Alertów
     ii. Zidentyfikowania wskaźników potencjalnego wystąpienia ataku
   - System ma pozwalać na wyeksportowanie wybranych zdarzeń w formacie CSV lub JSON
   - System ma zbierać informacje statystyczne odnośnie statusu podłączenia poszczególnych elementów do platformy zarządzania (sensorów i konektorów)
   - Wszelka aktywności w systemie winna być zapisywana i ewidencjonowana z zapewnieniem odpowiedniej rozliczalności działań analityków w środowisku
7. **Threat Intelligence** – system ma dostarczać i integrować dane zebrane przez producenta o zagrożeniach i kampaniach przestępczych

8. **Threat hunting** – system ma pozwalać na przeszukiwanie wszystkich danych zebranych z organizacji pod kątem różnych artefaktów:
    - Wyszukiwanie ma być realizowane z jednego miejsca dla wszystkich źródeł
    - System powinien pozwalać na wyszukiwanie po pełnej frazie (np. cała komenda) lub tylko fragmencie
    - System powinien pozwalać na wyszukiwanie artefaktu nawet jeśli nie jest znany atrybut powiązany z tym artefaktem np. wyszukanie ciągu, który mógłby zaistnieć jako wywołanie URL, fragment komendy, nazwa pliku itd.
    - W wyniku wyszukiwania system ma wskazywać linię czasu oraz powiązane ze zdarzeniem obiekty
    - Po zidentyfikowaniu obiektu system na pozwalać na odtworzenie przebiegu zdarzenia w łańcuchu przyczynowo-skutkowym. System ma pokazywać powiązania pomiędzy poszczególnymi zdarzeniami w łańcuchu
    - System powinien wyświetlać jak najpełniejsze dane odnośnie zdarzenia
    - Zdarzenia mają być mapowane, tam gdzie to możliwe, na techniki i taktyki MITRE ATT&CK (wskazanie konkretnego identyfikatora taktyki/techniki)
9. Incident response:
    - System w wyniku działań korelacyjnych ma tworzyć zagregowane alerty
    - System ma pozwalać o zarządzanie statusem alertu
    - System ma pozwalać na podejmowanie akcji w poszczególnych zdarzeniach
    - System ma pozwalać na tworzenie listy obiektów do zablokowania/listy wyjątków
10. **Specyfikacja technologiczna:**
    - Sensor EDR dedykowany na serwery ma integrować się z poniższymi platformami OS:
        i. **Windows 10**
        ii. **Windows Server 2019 (64-bit)**
        iii. **Windows Server 2016 (64-bit)**
        iv. **Windows Server 2012 / 2012 R2 (64-bit)**
        v. **Windows Server 2008 R2 (64-bit)**
        vi. **Red Hat Enterprise Linux 6 (64-bit)**
        vii. **Red Hat Enterprise Linux 7 (64-bit)**
        viii. **Red Hat Enterprise Linux 8 (64-bit)**
        ix. **CentOS Linux 6 (64-bit)**
        x. **CentOS Linux 7 (64-bit)**
        xi. **CentOS Linux 8 (64-bit)**
        xii. **Ubuntu 16 (64-bit)**
        xiii. **Ubuntu 18 (64-bit)**
        xiv. **Ubuntu 20 (64-bit)**

xv. **SLES Linux od ver. 11** xvi. **Oracle Linux 6** • System ma pozwalać na ciągłe kolekcjonowanie danych ze źródeł. W przypadku niedostępności stacji roboczej/serwera system ma zbierać dane lokalnie do momentu nawiązania kontaktu z konsolą • System ma być oparty o wydajny silnik analityczny pozwalający na pracę z danymi bez zbędnej zwłoki • **System powinien posiadać certyfikat potwierdzający zgodność przetwarzania danych z obowiązującymi standardami i dobrymi praktykami np. ISO27001.**

TABELA NR 1a – wymagania dodatkowe, punktowane.

WYMAGANIA FUNKCJONALNE DODATKOWO PUNKTOWANE
Opis wymagania
1. Oprogramowanie zabezpieczające musi umożliwiać agentową ochronę maszyn fizycznych i wirtualnych. Wszystkie funkcjonalności ochrony jak i EDR realizowane muszą być za pomocą **jednego agenta.**
2. **Wszystkie funkcjonalności** oprogramowania zabezpieczającego jak i EDR muszą być zarządzane **z tej samej konsoli**, za pomocą wspólnego interfejsu dostępnego z poziomu przeglądarki internetowej.
3. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność rekomendowania administratorowi uruchomienia konkretnych reguł monitorowania logów definiowanych i dostarczanych przez producenta oprogramowania.** Rekomendacja powinna być specyficzna dla konkretnego chronionego systemu. Rekomendacja powinna opierać się na cyklicznej, co najmniej raz na dobę analizie chronionego sytemu operacyjnego – jego wersji oraz zainstalowanym oprogramowaniu. Rekomendacja powinna dotyczyć co najmniej istotnych z punktu widzenia bezpieczeństwa logów.
4. **Oprogramowanie zabezpieczające musi mieć funkcjonalność rekomendowania administratorowi uruchomienia konkretnych reguł definiowanych i dostarczanych przez producenta Oprogramowania**. Rekomendacja powinna być specyficzna dla konkretnego chronionego systemu. Rekomendacja powinna opierać się na cyklicznej, przeprowadzanej co najmniej raz na dobę analizie chronionego systemu operacyjnego – jego wersji oraz zainstalowanym oprogramowaniu. Rekomendacja powinna dotyczyć, co najmniej elementów systemu operacyjnego, jakie należy monitorować pod kątem integralności (takie jak pliki, procesy);
5. Analiza podatności występujących na serwerze w celu wybrania i uruchomienia odpowiednich tzw. **wirtualnych poprawek musi być wykonywana w sposób automatyczny** co najmniej raz na dobę.

6. **Polityka w zakresie uruchamiana tzw. wirtualnych poprawek powinna być tworzona automatycznie**, indywidualnie da każdego chronionego zasobu bazując na analizie jego wersji, zainstalowanych poprawkach bezpieczeństwa i zainstalowanym oprogramowaniu. Taka analiza i optymalizacja polityki powinna być wykonywana co najmniej raz na dobę.

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

WARUNKI SERWISU – WYMAGANE PISEMNE OŚWIADCZENIA:
Wykonawca **zagwarantuje**, że przez okres **36 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**: a) nieautoryzowany dostęp, b) uszkodzenie, c) wykasowanie wszelkiego rodzaju oprogramowania, danych lub urządzeń peryferyjnych,
Wykonawca będzie również świadczył **usługę Wsparcia technicznego** (poza wsparciem technicznym producenta) przez okres **36 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. **Wsparcie techniczne dla systemu będzie obejmowało w szczególności**: - zapewnienie przez Wykonawcę kanału komunikacji pomiędzy Wykonawcą, a Zamawiającym, odpowiadającą za bieżącą obsługę systemu, rozwiązywanie 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 (kryterium oceny oferty)**. - 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/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/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 z wyszczególnieniem poszczególnych serwerów, w formie elektronicznej i papierowej, w ilości 3 egzemplarzy dla każdej z wymienionych form, wraz z instrukcjami jego obsługi w podziale na: • dokumentacja techniczna środowiska objętego ochroną wraz z wyspecyfikowaniem zastosowanych reguł/ polityk bezpieczeństwa, • instrukcja obsługi dla operatora, • instrukcja obsługi dla administratora.

Wraz ze zgłoszeniem przystąpienia do odbioru końcowego systemu Wykonawca **dostarczy dokument poświadczający udzielenie 36 miesięcznej gwarancji**, wsparcia technicznego oraz wszystkie niezbędne licencje potwierdzające zgodne z prawem nabycie systemu przez **Zamawiającego**.
Zakończenie wdrożenia systemu winno być **udokumentowane raportem końcowym** wygenerowanym po zakończeniu procesu wdrożenia, **dokumentującym status bezpieczeństwa serwerowego środowiska teleinformatycznego**.

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

Zamawiający nie dopuszcza składanie ofert częściowych.

II. TERMIN WYKONANIA PRZEDMIOTU ZAMÓWIENIA: 1 miesiąc 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 cześć 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 – 56%
2. Doświadczenie – 10 pkt
3. Świadczenie usług wsparcia technicznego – 6 pkt
4. Wymagania funkcjonalne dodatkowo punktowane z TABELI NR 1a – 18 pkt
5. Jakość - umiejscowienie oferowanego systemu w danej ćwiartce Gartner Magic Quadrant for Endpoint Protection Platforms – 10 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:

$$\text{Ocena oferty X} = \frac{\text{Wartość brutto oferty najtańszej w danym zadaniu}}{\text{Wartość brutto oferty ocenianej w danym zadaniu}} \times 56\ \%$$

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 przypadała na lata 2016 - 2021. 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 „Świadczenie usług wsparcia technicznego”: Maksymalna ilość punktów jaką można uzyskać w okresie świadczenia gwarancji:

Pakiet 50 godzin serwisowych rocznie – 0 pkt.
Pakiet 150 godzin serwisowych rocznie – 3 pkt.
Pakiet 200 godzin serwisowych rocznie – 6 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”: 6 pkt w danej części.

Ad.4. Kryterium „Wymagania funkcjonalne dodatkowo punktowane z TABELI NR 1a”: Maksymalna ilość punktów jaką można uzyskać to 18 pkt tj. po 3 pkt za każde wymaganie.

Opis wymagania	Ilość pkt jeśli oprogramowanie spełnia wymaganie
1. Oprogramowanie zabezpieczające musi umożliwiać agentową ochronę maszyn fizycznych i wirtualnych. Wszystkie funkcjonalności ochrony jak i EDR realizowane muszą być za pomocą **jednego agenta.**	**3**
2. **Wszystkie funkcjonalności** oprogramowania zabezpieczającego jak i EDR muszą być zarządzane **z tej samej konsoli**, za pomocą wspólnego interfejsu dostępnego z poziomu przeglądarki internetowej.	**3**
3. Oprogramowanie zabezpieczające musi posiadać **funkcjonalność rekomendowania administratorowi uruchomienia konkretnych reguł monitorowania logów definiowanych i dostarczanych przez producenta oprogramowania.** Rekomendacja powinna być specyficzna dla konkretnego chronionego systemu. Rekomendacja powinna opierać się na cyklicznej, co najmniej raz na dobę analizie chronionego sytemu operacyjnego – jego wersji oraz zainstalowanym oprogramowaniu. Rekomendacja powinna dotyczyć co	**3**

najmniej istotnych z punktu widzenia bezpieczeństwa logów.	
4. **Oprogramowanie zabezpieczające musi mieć funkcjonalność rekomendowania administratorowi uruchomienia konkretnych reguł definiowanych i dostarczanych przez producenta Oprogramowania**. Rekomendacja powinna być specyficzna dla konkretnego chronionego systemu. Rekomendacja powinna opierać się na cyklicznej, przeprowadzanej co najmniej raz na dobę analizie chronionego systemu operacyjnego – jego wersji oraz zainstalowanym oprogramowaniu. Rekomendacja powinna dotyczyć, co najmniej elementów systemu operacyjnego, jakie należy monitorować pod kątem integralności (takie jak pliki, procesy);	**3**
5. Analiza podatności występujących na serwerze w celu wybrania i uruchomienia odpowiednich tzw. **wirtualnych poprawek musi być wykonywana w sposób automatyczny** co najmniej raz na dobę.	**3**
6. **Polityka w zakresie uruchamiana tzw. wirtualnych poprawek powinna być tworzona automatycznie**, indywidualnie da każdego chronionego zasobu bazując na analizie jego wersji, zainstalowanych poprawkach bezpieczeństwa i zainstalowanym oprogramowaniu. Taka analiza i optymalizacja polityki powinna być wykonywana co najmniej raz na dobę.	**3**

Ad.5. Kryterium „jakościowe - umiejscowienie oferowanego systemu w danej ćwiartce, najnowszego na dzień złożenia oferty, raportu Gartner Magic Quadrant for Endpoint Protection Platforms”
Za u umiejscowienie oferowanego produktu w danej ćwiartce Gartner Magic Quadrant for Endpoint Protection Platforms, przypisuje się odpowiednią liczbę kryterium jakości:

- na poziomie Leaders -10 punktów
- na poziomie Challengers - 5 punktów
- na poziomie Visioners - 2 punkty
- na poziomie Niche Players lub brak podania w formularzu poziomu - 0 punktów

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 listopada 2021 r. do godz. 13^{00}**
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

„Wdrożenie zabezpieczeń serwerowego środowiska teleinformatycznego - NI-I-9/2021”

Nie otwierać przed dniem 10 listopada 2021 r. do godz. 13^{15}”;

oraz nazwą Wykonawcy.

Otwarcie ofert nastąpi w siedzibie Zamawiającego - Białystok, ul. Młynowa 52/1 **w dniu 10 listopada 2021 r. do godz.13^{15} świetlica.**

„Wodociągi Białostockie” Sp. z o.o. w związku z sytuacją epidemiologiczną otwarcia ofert będą się odbywały bez udziału Wykonawców (osób trzecich). Informacje dotyczące otwarcia ofert zostaną zamieszczane niezwłocznie na stronie bip.wobi.pl.

X. TERMIN ZWIĄZANIA OFERTĄ

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 zwięzłe 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 dowidział 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 – Projekt umowy

Z poważaniem

……

podpis Zamawiającego

Załącznik Nr 3 RODO

Nr ref. sprawy: NI–I–9/2021

Dot.: Wdrożenie zabezpieczeń serwerowego środowiska teleinformatycznego.

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 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,
- 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**.

……

---

* ***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 7 /NI/ 2021

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. Jarosława Poniatowicza – Wiceprezesa Zarządu;

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 **wdrożenie zabezpieczeń serwerowego środowiska teleinformatycznego:**

Wykonawca:

a) dostarczy i zainstaluje system zabezpieczeń serwerowego środowiska teleinformatycznego, który obejmie swoim zasięgiem 55 serwerów wirtualnych i maszyn fizycznych. 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 we współpracy z **Zamawiający** integrację oferowanego rozwiązania z posiadanym przez Zamawiającego systemem SecureVisio (ESECURE SP. Z O.O., ul. Hoffmanowej 19, PL-35016 Rzeszów) w celu dostarczania informacji o stanie bezpieczeństwa serwerów, tak by system SecureVisio był w stanie zidentyfikować oraz wykorzystać te dane w korelacjach dotyczących Reguł Bezpieczeństwa,
d) przeprowadzi szkolenie z obsługi i administracji wdrożonego systememu 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 odbioru **raport dokumentującym status bezpieczeństwa serwerowego środowiska teleinformatycznego** 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** z wyszczególnieniem poszczególnych serwerów, w formie elektronicznej i papierowej, w ilości 3 egzemplarzy dla każdej z wymienionych form, wraz z instrukcjami jego obsługi w podziale na:
    - dokumentacja techniczna środowiska objętego ochroną wraz z wyspecyfikowaniem zastosowanych reguł/ polityk bezpieczeństwa,
    - 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 1 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 przekaże **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, zamienne 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 przekaże **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** przekaże 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**

   Pan ……tel: ……e-mail: ……

   b) ze strony **Wykonawcy**

   Pan ……tel: ……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 **……3…. (*…36 m-cy……..*) 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 **…3… (*……36 m-cy….*) 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 ……3…….. 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 jakiejkolwiek osobie trzeciej (informacje poufne).

2. **Strony** gwarantują zachowanie poufności danych i zobowiązują się w szczególności do :
   - nie ujawniania w jakiejkolwiek formie informacji poufnych dotyczących wszystkich aspektów współpracy dotyczących realizacji Umowy jakiejkolwiek 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 widomości 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 ***„Wdrożenie zabezpieczeń serwerowego środowiska teleinformatycznego”,***
    b) Załącznik nr 2 – **Oświadczenie Wykonawcy dotyczące możliwości pozyskania kodów źródłowych wdrażanego systemu**,
    c) Załącznik nr 3 – **Oferta Wykonawcy**.
9. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze **Stron**.

ZAMAWIAJĄCY	**WYKONAWCA**
……..…	……
……..	……