GÓRNOŚLĄSKIE
PRZEDSIĘBIORSTWO
WODOCIĄGÓW
SPÓŁKA AKCYJNA

ZK/024/258W/2025

Katowice, dnia 23 czerwca 2025 r.

WYKONAWCY
w postępowaniu o udzielnie zamówienia
Nr ZK/024/251W/2025

Górnośląskie Przedsiębiorstwo Wodociągów Spółka Akcyjna w odpowiedzi na pytania skierowane przez Wykonawcę ubiegającego się o udzielenie zamówienia, prowadzonego w trybie zapytania ofertowego poprzez skierowanie zaproszenia do składania ofert do Wykonawców, umieszczenie zaproszenia na stronie internetowej GPW S.A. w Katowicach, w oparciu o art. 52 ust 1 pkt 1 i 2 w zw. z art. 51 ust. 2 pkt 3 Regulaminu Udzielania Zamówień przez Górnośląskie Przedsiębiorstwo Wodociągów S.A. z siedzibą w Katowicach (dalej „Regulamin"), w celu wyłonienia Wykonawcy na realizację usługi pn.: **„Przeprowadzenie u Zamawiającego jako operatora usługi kluczowej audytu w zakresie zgodności z ustawą o Krajowym Systemie Cyberbezpieczeństwa z uwzględnieniem dyrektywy NIS2 oraz wdrożenie systemu zarządzania bezpieczeństwem informacji zgodnie z ustawą o Krajowym Systemie Cyberbezpieczeństwa oraz wymaganiami dyrektywy NIS2 w Górnośląskim Przedsiębiorstwie Wodociągów S.A. w Katowicach"** (*postępowanie Nr **ZK/024/251W/2025*** z dnia 12 czerwca 2025 roku – data publikacji na stronie) w oparciu o art. 38 ust. 1 Regulaminu udziela następujących wyjaśnień:

Treść zapytania dostarczonego Zamawiającemu w wiadomości e-mail w dniu 17 czerwca 2025 roku: *„W ramach audytu zgodności z ustawą o Krajowym Systemie Cyberbezpieczeństwa prosimy o doprecyzowanie zakres audytu infrastruktury, ze szczególnym uwzględnieniem części technologicznej (OT – Operational Technology):*

Lista pytań OT:

1. *Liczba lokalizacji objętych audytem części technologicznej, wraz z ich charakterystyką (np. zakład produkcyjny, obiekt liniowy, zewnętrzna stacja technologiczna) oraz jednoznaczne określenie granic audytu dla każdej z tych lokalizacji. Proszę określić zakres, który może obejmować m.in. systemów monitoringu wizyjnego (CCTV), instalacji alarmowych, systemów kontroli dostępu oraz urządzeń z obszaru automatyki budynkowej i sensoryki (np. inteligentnych czujników, urządzeń komunikujących się przez fieldbus, IO-Link itp.).*
2. *Przybliżona liczba urządzeń objętych audytem, dla których zidentyfikowano znane podatności (CVE), a także informacja, czy w ramach audytu planowane jest przeprowadzenie inwentaryzacji tych urządzeń z uwzględnieniem ich rozmieszczenia w strukturze technologicznej (OT).*
3. *Wykaz wykorzystywanych protokołów komunikacyjnych stosowanych w infrastrukturze OT oraz określenie rzeczywistej topologii połączeń między urządzeniami.*

4. *Specyfikacja standardów przemysłowych obowiązujących w środowisku audytowanym. Proszę wskazać stosowane normy i wytyczne dotyczące bezpieczeństwa systemów automatyki przemysłowej (np. IEC 62443), a także standardy komunikacyjne wykorzystywane w systemach sterowania (takie jak Modbus TCP, PROFINET, DNP3, OPC UA, EtherNet/IP). W zakresie tym należy również uwzględnić wewnętrzne regulacje, polityki, które wpływają na sposób zarządzania infrastrukturą OT.*
5. *Informacje na temat systemów SCADA/HMI oraz ich integracji z pozostałymi komponentami infrastruktury.*
6. *Planowane metody pozyskiwania danych.*
7. *Oczekiwany poziom zgodności audytu z wymaganiami norm przemysłowych, a także zasady raportowania i dokumentowania wyników, w tym odniesienie do ustawy o Krajowym Systemie Cyberbezpieczeństwa. Proszę określić, czy audyt ma w pełni uwzględniać wymagania konkretnej normy, np. IEC 62443, w kontekście wdrożenia modelu referencyjnego Purdue – w szczególności w zakresie segmentacji sieci, podziału stref i poziomów bezpieczeństwa, kontroli dostępu oraz zarządzania komunikacją pomiędzy warstwami.*
8. *Preferowane okna czasowe przeprowadzenia audytu, uwzględniające specyfikę i harmonogram procesów produkcyjnych.*
9. *Oczekiwania dotyczące formy i szczegółowości końcowego raportu, wraz z rekomendacjami technicznymi i organizacyjnymi.*

Lista pytań IT:

1. *Czy Zamawiający może podać liczbę urządzeń podlegających audytowi, z rozbiciem na lokalizacje oraz typ funkcji (np. firewall, router, przełącznik L2/L3, kontroler WLAN, serwer syslog/SIEM/SOC)?*
2. *Czy Zamawiający może wskazać dostawców (vendorów) sprzętu objętego audytem?*
3. *Czy Zamawiający może określić, czy przewiduje dostęp zdalny do urządzeń, czy też będzie wymagana weryfikacja fizyczna we wskazanych lokalizacjach?*
4. *Czy Zamawiający może określić, co chciałby otrzymać w raporcie końcowym inwentaryzacji (np. listę sprzętu, listę zainstalowanego oprogramowania, listę plików audio/wideo itp.)?*
5. *Czy Zamawiający może określić, czy posiada centralne zarządzanie konfiguracjami urządzeń (np. FortiManager, Cisco DNA Center, Ansible)? Jeśli tak, czy Zamawiający może podać narzędzie i jego wersję?*
6. *Czy Zamawiający może wskazać, czy posiada dokumentację techniczną rozwiązań, zawierającą informacje o środowisku, takie jak topologia podłączeń lub schematy?*
7. *Czy Zamawiający może wskazać, czy posiada spis metodyki dostępu do urządzeń (np. adresy IP, konta, poświadczenia, ewentualne procedury MFA)?*
8. *Czy Zamawiający może określić, czy zostanie zapewniony dostęp zdalny do audytowanego środowiska (serwery, serwery wirtualne, komputery, stacje robocze, urządzenia sieciowe, systemy backupu itp.)?*
9. *Czy Zamawiający może wskazać, gdzie i w jakiej formie gromadzone są logi i zdarzenia (events)? Czy Zamawiający może podać dostawcę centralnego systemu (syslog, SIEM) oraz okres czasowy, który ma podlegać weryfikacji?*
10. *Czy Zamawiający może określić, jakie konkretnie logi mają podlegać audytowi?*

11. *Czy Zamawiający może wskazać, ile systemów monitorowania jest wdrożonych w infrastrukturze IT i jakie to systemy?*
12. *Czy Zamawiający może określić, jakie uprawnienia otrzyma audytor? Czy Zamawiający może doprecyzować, czy audytor będzie miał konta administratora, czy też konieczne będą sesje z lokalnym personelem?*
13. *Czy Zamawiający może doprecyzować zakres „kontroli dostępu" w kontekście oceny struktury sieci: czy chodzi o reguły warstwy 3 (ACL, firewall policy), czy o inne mechanizmy (np. 802.1X, NAC)?*
14. *Czy Zamawiający może określić, czy w odniesieniu do punktu „antywirusy" ma na myśli zabezpieczenia na urządzeniach sieciowych (np. ATP/UTM), czy rozwiązania endpoint security? Jeśli to drugie, czy Zamawiający może wskazać producenta?*
15. *Czy Zamawiający może określić, ile stacji roboczych i jakich producentów (vendorów) ma podlegać audytowi?*
16. *Czy Zamawiający może określić, ile i jakie serwery mają podlegać audytowi?*
17. *Czy Zamawiający może wskazać, czy w infrastrukturze IT wdrożona jest usługa katalogowa Active Directory? Czy Zamawiający może określić, czy audytowi ma podlegać cała infrastruktura AD?*
18. *Czy Zamawiający może przedstawić wykaz lokalizacji z wyszczególnieniem ilości sprzętu w każdej z nich, uwzględniającym wskazane grupy urządzeń (serwery, serwery wirtualne, komputery, stacje robocze, urządzenia sieciowe, systemy backupu itp.)?*
19. *Czy Zamawiający może określić, z jakich systemów operacyjnych korzystają serwery, serwery wirtualne, komputery i stacje robocze?*
20. *Czy Zamawiający może wskazać, w jakich dniach i godzinach będziemy mieli fizyczny dostęp do lokalizacji?*
21. *Czy Zamawiający może potwierdzić, czy posiada wdrożony system MFA?*
22. *Czy Zamawiający może potwierdzić, czy posiada wdrożony system SSO?*
23. *Czy Zamawiający może wskazać, czy są wdrożone polityki dotyczące złożoności i wymiany haseł?*
24. *Czy Zamawiający może określić, czy korzysta z VDI? Jeśli tak, czy Zamawiający może podać ilość?*
25. *Czy Zamawiający może wskazać, czy do środowiska mają dostęp firmy trzecie (podwykonawcy, partnerzy etc.)?*
26. *Czy Zamawiający może wskazać, czy są wdrożone i określone polityki backupu?*
27. *Czy Zamawiający może określić, z jakiego systemu do wykonywania i zarządzania kopiami zapasowymi Państwo korzystają?*
28. *Czy Zamawiający może wskazać, czy kopie są wynoszone poza główną lokalizację backupu?*
29. *Czy Zamawiający może potwierdzić, czy są przeprowadzane testowe odtworzenia?*
30. *Czy Zamawiający może wskazać, czy są określone i wdrożone mechanizmy retencji?*
31. *Czy Zamawiający może określić, jaki sprzęt jest wykorzystywany w obszarze backupu?*
32. *Czy Zamawiający może podać, jaki jest obecnie wykorzystywany system kopii zapasowych, w jakiej wersji oraz jaki typ licencjonowania?*

33. *Czy Zamawiający może wskazać, czy obecnie jest lub docelowo będzie wykorzystywany mechanizm szyfrowania kopii zapasowych przy replikacji?*
34. *Czy Zamawiający może określić, jaka jest całkowita zajmowana przestrzeń przez obecne środowisko kopii zapasowych?*
35. *Czy Zamawiający może podać, jaka jest retencja na zabezpieczanych środowiskach?*
36. *Czy Zamawiający może wskazać, czy jest obecnie uruchomiony mechanizm weryfikacji kopii zapasowych - manualnie lub automatycznie?*
37. *Czy Zamawiający może podać, jaki wirtualizator oraz w jakiej wersji jest u Państwa wykorzystywany produkcyjnie?*
38. *Czy Zamawiający może określić, ile maszyn wirtualnych znajduje się w środowisku produkcyjnym, które jest objęte kopią zapasową? ".*

Odpowiedź Zamawiającego:

W nawiązaniu do treści wiadomości e-mail z dnia 17 czerwca 2025 roku (data wysłania wiadomości e-mail przez Wykonawcę) Zamawiający udziela następującej odpowiedzi:

Zamawiający informuje, iż zadane pytania w większości mają charakter szczegółowy i dotyczą informacji technicznych nt. wykorzystywanych systemów, rozwiązań bezpieczeństwa oraz ich topologii. Na obecnym etapie Zamawiający może udzielić odpowiedzi na pytania, które nie wymagają dostępu do szczegółowych danych technicznych.

Lista pytań OT:

Ad.1) Audyt obejmować będzie systemy automatyki przemysłowej (bez systemów CCTV, kontroli dostępu, automatyki budynkowej itp), zlokalizowanych w 13 obiektach Zamawiającego (Zakłady Uzdatniania Wody, Stacje Uzdatniania wody, siedziba Spółki).
Ad.2) 46 stacji roboczych. Audyt winien być przeprowadzony zgodnie z ustawą o Krajowym Systemie Cyberbezpieczeństwa z uwzględnieniem dyrektywy NIS2.
Ad.6) Planowane metody pozyskiwania danych obejmują wizje lokalne oraz pasywne skanowanie sieci.
Ad.7) Oczekiwany poziom zgodności audytu z wymaganiami norm przemysłowych oraz zasady raportowania i dokumentowania wyników są określone przez ustawę o Krajowym Systemie Cyberbezpieczeństwa oraz dyrektywę NIS2. Audyt ma w pełni uwzględniać wymagania tej ustawy i dyrektywy.
Ad.8) Preferowane okna czasowe przeprowadzenia audytu, uwzględniające specyfikę i harmonogram procesów produkcyjnych, to dni robocze w godzinach 9:00-13:00.
Ad.9) Audyt ma zostać przeprowadzony zgodnie z wymaganiami ustawy KSC oraz dyrektywy NIS 2.

Lista pytań IT:

Ad.3) Zamawiający wymaga weryfikacji fizycznej we wskazanych lokalizacjach.
Ad.4) Zamawiający oczekuje przeprowadzenia czynności audytowych zgodnie wymaganiami ustawy KSC oraz dyrektywy NIS 2.
Ad.12) Zamawiający dopuszcza wyłącznie sesje pod nadzorem personelu.

Ad.18) Wykaz lokalizacji zostanie udostępniony Wykonawcy po podpisaniu umowy.

Ad.20) Czynności audytowe mogą być prowadzone w dni robocze w godzinach 9:00-13:00.

Dyrektor
Pionu Organizacyjnego
Dorota Gardoń

Rozdzielnik:

1. Strona internetowa.
2. aa.

Osoba do kontaktu; Dorota Gardoń – Dyrektor Pionu Organizacyjnego, tel. 32 60 38 888
e-mail: d.gardon@gpw.katowice.pl