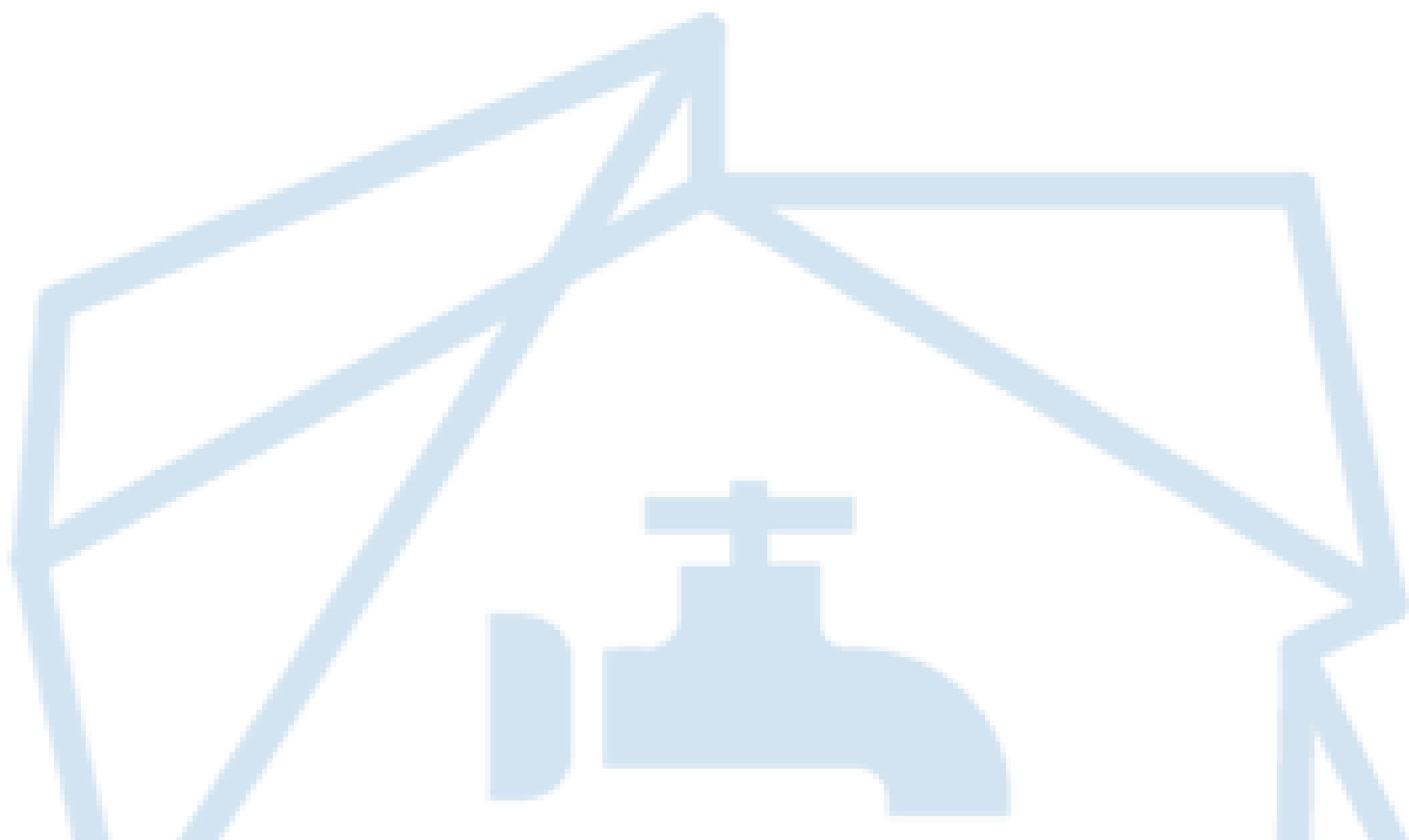


OPIS PRZEDMIOTU ZAMÓWIENIA

CZĘŚĆ JAWNA

W postępowaniu pn.: Budowa odporności na cyberataki w Prochowickim Przedsiębiorstwie
Komunalnym Sp. z o.o. w Prochowicach"



1. INFORMACJE OGÓLNE

- 1.1. **Przedmiotem zamówienia jest kompleksowa realizacja zadań mających na celu zwiększenie cyberbezpieczeństwa Zamawiającego w ramach Projektu grantowego w przedsięwzięciu pn. „Cyberbezpieczne wodociągi” w celu osiągnięcia zadeklarowanego we wniosku grantowym przyrostu poziomu bezpieczeństwa.**
- 1.2. W ramach Przedmiotu zamówienia Zamawiający przewiduje realizację zadań we wskazanych poniżej obszarach¹:
- 1.2.1. **obszar organizacyjny**, który obejmuje wszelkie aspekty organizacyjne bezpieczeństwa systemów teleinformatycznych IT i OT, tj. audyt bezpieczeństwa, audyt zgodności z przepisami i normami, opracowanie, wdrożenie, utrzymanie i aktualizacja systemu zarządzania bezpieczeństwem informacji, systemu zarządzania bezpieczeństwem systemu teleinformatycznego IT/OT, systemu zarządzania ciągłością działania systemu teleinformatycznego IT/OT;
- 1.2.2. **obszar kompetencyjny**, który obejmuje wszelkie działania podnoszące świadomość, wiedzę i umiejętności na poziomie podstawowym, kierowniczym i specjalistycznym w zakresie cyberbezpieczeństwa, realizowane dla pracowników podmiotu, operatorów i administratorów systemów teleinformatycznych IT/OT, kadry kierowniczej IT/OT, kadry kierowniczej i zarządzającej podmiotu;
- 1.2.3. **obszar techniczny** (dotyczy obszaru funkcjonalnego IT i wspólnego z OT), który obejmuje wszelkie komputerowe środki techniczne – sprzętowe i aplikacyjne – służące do zabezpieczenia i zapewnienia bezpieczeństwa komponentów środowiska teleinformatycznego IT, tj.: stacje robocze, serwery, dane biznesowe, oprogramowanie biznesowe, systemy pamięci masowej, urządzenia sieciowe środowisko sieciowe IT i wspólne z OT;
- 1.2.4. **obszar techniczny OT** (dotyczy obszaru funkcjonalnego OT), który obejmuje wszelkie komputerowe środki techniczne i wybrane elektrotechniczne środki techniczne – sprzętowe i aplikacyjne – służące do zabezpieczenia i zapewnienia bezpieczeństwa w zakresie zbiorowego zaopatrzenia w wodę i zbiorowego odprowadzania ścieków, tj. komponentów środowiska teleinformatycznego OT/ICS/IloT i środowiska IT obszaru przemysłowego OT, w tym: stacje robocze, serwery, dane systemów IT/OT/ICS/IloT, systemy IT/OT/ICS/IloT, oprogramowanie IT/OT/ICS/IloT, urządzenia sieciowe i środowisko sieciowe IT/OT/ICS/IloT oraz obejmuje rozwiązania zabezpieczenia systemów bezpieczeństwa wizyjnego, fizycznego i technicznego.

¹ Zgodnie z Regulaminem Konkursu Grantowego pn. „Cyberbezpieczne wodociągi” dostępnym na stronie naboru: <https://www.gov.pl/web/cppc/start-naboru-cyberbezpieczne-wodociagi> [dostęp: 07.01.2026 r.]

- 1.3. Dla każdego z obszarów, o których mowa w pkt 1.2, Zamawiający przewidział szczegółowy zakres niezbędnych do dostawy i wdrożenia produktów, działań i usług bezpieczeństwa, pogrupowanych w konkretne Rozwiązania. Podział ten jest zgodny z „Formularzem potwierdzającym realną propozycję zwiększenia odporności” będącym załącznikiem do Wniosku o przyznanie grantu w ramach Projektu grantowego w przedsięwzięciu pn. „Cyberbezpieczne wodociągi”, obowiązującym na dzień złożenia Wniosku przez Zamawiającego.
- 1.4. Opis stanu obecnego oraz planowanego wzrostu cyberbezpieczeństwa jaki ma być osiągnięty w wyniku realizacji Przedmiotu Zamówienia został przedstawiony Formularzu potwierdzającym realną propozycję zwiększenia odporności w wyniku realizacji Projektu grantowego („Formularz oceny skuteczności”) stanowiącym Załącznik do OPZ części niejawnej. Dla każdego z rozwiązań obszarowych wskazano minimalny wymagany stan docelowy, który musi zostać osiągnięty w ramach udzielonego Zamówienia.
- 1.5. Wykonawca zobowiązany jest do dostarczenia, wdrożenia i uruchomienia wszystkich rozwiązań w zakresie nie mniejszym niż opisany w poszczególnych arkuszach przedstawionych w Formularzu potwierdzającym realną propozycję zwiększenia odporności w wyniku realizacji Projektu grantowego („Formularz oceny skuteczności”), wraz z zapewnieniem kompletności, spójności, interoperacyjności oraz pełnej funkcjonalności wdrożenia.
- 1.6. Zamawiający wymaga, aby Przedmiot Zamówienia został zrealizowany jako jedno, zintegrowane i spójne przedsięwzięcie obejmujące obszar organizacyjny, kompetencyjny, techniczny IT oraz techniczny OT, w pełnym zakresie funkcjonalnym, zapewniającym wysoki poziom bezpieczeństwa oraz wysoki stopień pokrycia poszczególnych obszarów bezpieczeństwa.
- 1.7. W szczególności Zamawiający wymaga, aby:
 - 1.7.1. wyniki audytów, analiz, inwentaryzacji, oceny ryzyka i oceny zgodności w obszarze organizacyjnym stanowiły bezpośrednią podstawę do konfiguracji i wdrożenia środków technicznych oraz organizacyjnych w obszarze IT i OT;
 - 1.7.2. opracowywane i wdrażane systemy zarządzania bezpieczeństwem informacji, bezpieczeństwem systemów teleinformatycznych IT/OT oraz ciągłości działania pozostawały w pełnej zgodności z wdrażaną architekturą techniczną, przyjętymi procedurami operacyjnymi, zasadami administracji oraz sposobem eksploatacji środowiska IT i OT;
 - 1.7.3. szkolenia realizowane w ramach Przedmiotu Zamówienia były oparte na rzeczywiście wdrażanych lub wdrożonych u Zamawiającego procedurach, konfiguracjach, narzędziach, architekturze oraz modelu organizacyjnym, a nie miały charakteru ogólnego lub oderwanego od wdrożonych rozwiązań;

- 1.7.4. rozwiązania sprzętowe i programowe wdrażane w obszarze IT oraz OT były wzajemnie kompatybilne, interoperacyjne i dostosowane do wymagań wynikających z wdrażanych systemów zarządzania, procedur bezpieczeństwa, zasad nadzoru, monitoringu, reagowania na incydenty oraz utrzymania ciągłości działania;
- 1.7.5. wszystkie elementy techniczne i organizacyjne funkcjonowały jako jedna spójna architektura bezpieczeństwa, obejmująca co najmniej integracje pomiędzy systemami, korelację i centralizację logów, synchronizację czasu, spójne zasady uwierzytelniania i autoryzacji, jednolite mechanizmy monitorowania
- 1.7.6. wdrożenie w obszarze IT i OT uwzględniało wzajemne zależności pomiędzy środowiskami, w szczególności na styku systemów biznesowych, systemów przemysłowych, systemów zdalnego dostępu, systemów nadzoru, systemów transmisji danych oraz systemów bezpieczeństwa fizycznego, technicznego i wizyjnego;
- 1.7.7. odpowiedzialność za osiągnięcie docelowego efektu bezpieczeństwa, zgodności, integralności architektury, poprawności integracji oraz skuteczności wdrożenia spoczywała na jednym wykonawcy lub konsorcjum występującym jako jeden wykonawca, zdolnym do zapewnienia jednolitego modelu realizacji, koordynacji i odpowiedzialności za rezultat.
- 1.8. Zamawiający oczekuje, aby wszystkie elementy Przedmiotu Zamówienia były realizowane w zgodności z Komunikatem pełnomocnika rządu ds. cyberbezpieczeństwa w sprawie ataków na przemysłowe systemy sterowania (ICS/OT) z 24 lutego 2025 r.
- 1.9. Zamawiający wymaga, aby Przedmiot Zamówienia był realizowany zgodnie z aktualnym stanem wiedzy technicznej, normami i aktami normatywnymi.
- 1.10. Zamawiający wymaga, aby sprzęt będący Przedmiotem Zamówienia był nowy, nieużywany i wyprodukowany nie wcześniej niż 12 miesięcy od dnia dostawy.
- 1.11. **Wszelkie urządzenia dostarczane w ramach Przedmiotu Zamówienia muszą być objęte wsparciem producenta przez okres nie mniejszy niż 36 miesięcy od dnia dostawy w pełnym zakresie funkcjonalnym, nie wymagającym ponoszenia dodatkowych nakładów finansowych przez Zamawiającego innych niż wymienione w formularzu ofertowym.**
- 1.12. **Oprogramowanie musi być dostarczone i zainstalowane w wersji aktualnej (stabilnej) na dzień jego instalacji.**
- 1.13. **Oprogramowanie musi być oferowane w modelu zapewniającym Zamawiającemu bezterminowe prawo do korzystania. Dopuszcza się w szczególności licencje wieczyste oraz rozwiązania open source. Nie dopuszcza się modeli subskrypcyjnych, jeżeli po upływie okresu subskrypcji Zamawiający traci prawo do dalszego legalnego korzystania z oprogramowania. Dopuszcza się model subskrypcyjny wyłącznie w zakresie aktualizacji sygnatur IPS/IDS oraz usług lub funkcjonalności typu XDR/EDR, o ile wygaśnięcie subskrypcji nie pozbawia Zamawiającego prawa do korzystania z bazowego**

oprogramowania, a jedynie powoduje utratę dostępu do aktualizacji, nowych sygnatur, feedów, usług chmurowych lub funkcji analitycznych świadczonych w modelu czasowym.

- 1.14. W ramach realizacji Przedmiotu Zamówienia Wykonawca ma obowiązek przeprowadzić analizę przedwdrożeniową.
- 1.15. W ramach prowadzonych prac, a w szczególności prac konfiguracyjnych, Zamawiający oczekuje utrzymania funkcjonalności wszystkich posiadanych przez siebie systemów i aplikacji. Prace wdrożeniowe muszą być przeprowadzone w taki sposób, aby nie zakłócić normalnej pracy Zamawiającego.
- 1.16. Jeżeli podczas prowadzonych prac zaistnieje konieczność rekonfiguracji posiadanych przez Zamawiającego systemów, Wykonawca jest zobowiązany dokonać takich rekonfiguracji na własną odpowiedzialność oraz własny koszt.
- 1.17. Wykonawca dokona instalacji, konfiguracji, parametryzacji i integracji dostarczanego sprzętu i oprogramowania.
- 1.18. Wykonawca ma obowiązek dostarczyć dokumentację powdrożeniową zawierającą co najmniej opisy wdrożenia, opisy konfiguracji, instrukcje obsługi, wykaz haseł, dostępów.
- 1.19. Dokumentacja musi być spójna i zapewniać zgodność z wymaganiami SZBI i SZCD.
- 1.20. W ramach realizacji Przedmiotu Zamówienia wykonawca dokona wszelkich prac konfiguracyjnych, technicznych i wdrożeniowych niezbędnych do zapewnienia celu Projektu Grantowego.
- 1.21. Opis stanu obecnego oraz szczegółowe wymagania Zamawiającego w tym specyfikację przyjętych Rozwiązań umieszczono w części OPZ stanowiącą informacje chronione.