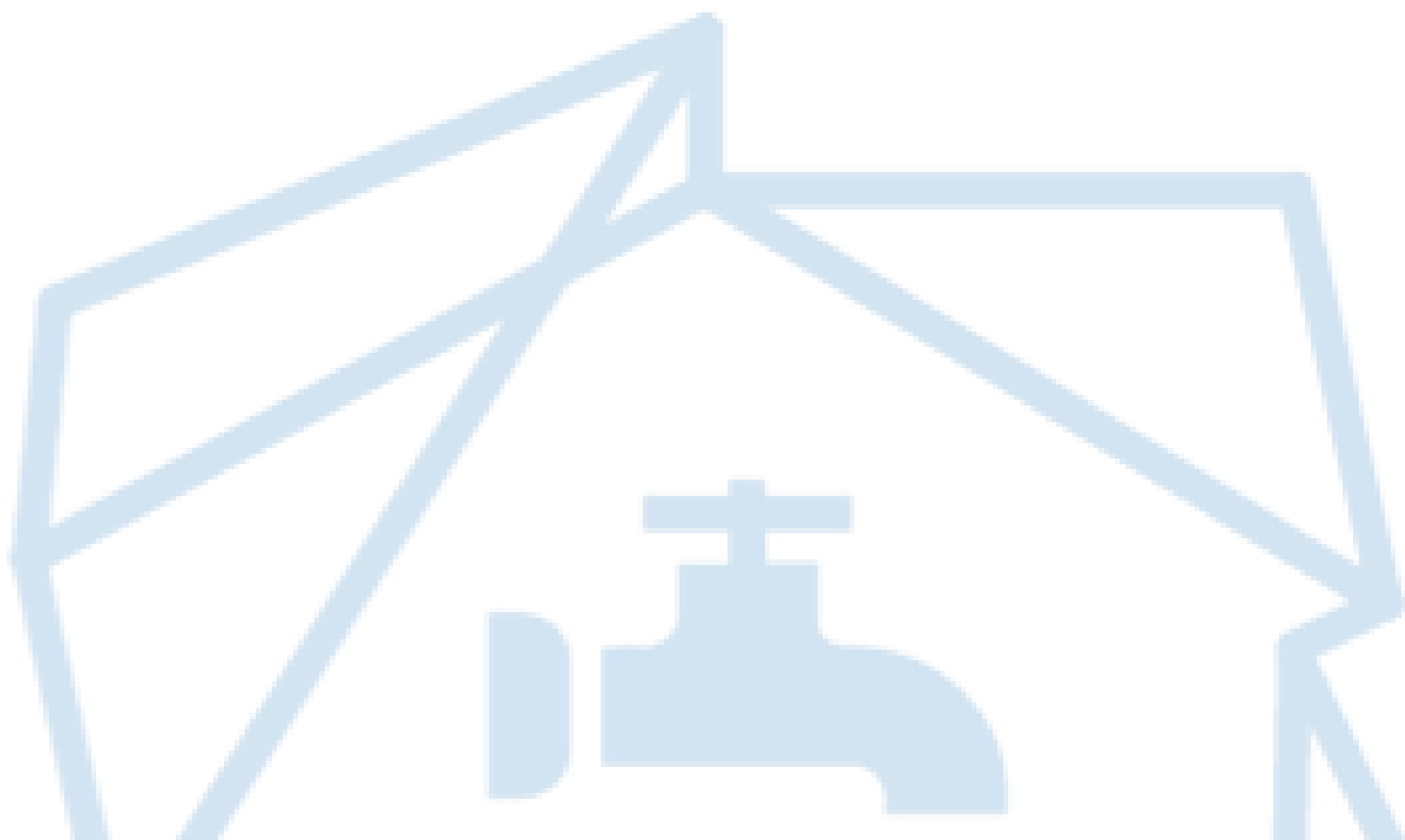


## OPIS PRZEDMIOTU ZAMÓWIENIA

### CZĘŚĆ JAWNA

W postępowaniu pn.: Kompleksowe przygotowanie i realizacja przedsięwzięć zwiększających cyberbezpieczeństwo w ramach projektu grantowego pn. „Projekt poprawy odporności infrastruktury IT i OT w GTKOM Sp. z o.o. w Tczewie”



## 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”.
- 1.2. W ramach Przedmiotu zamówienia Zamawiający przewiduje realizację zadań we wskazanych poniżej obszarach<sup>1</sup>:
  - 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 IT** (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;
  - 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/IIoT i środowiska IT obszaru przemysłowego OT, w tym: stacje robocze, serwery, dane systemów IT/OT/ICS/IIoT, systemy IT/OT/ICS/IIoT, oprogramowanie IT/OT/ICS/IIoT, urządzenia sieciowe i środowisko sieciowe IT/OT/ICS/IIoT oraz obejmuje rozwiązania zabezpieczenia systemów bezpieczeństwa wizyjnego, fizycznego i technicznego.
- 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,

---

<sup>1</sup> 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.]

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. Część 2 oraz opis stanu obecnego oraz szczegółowe wymagania Zamawiającego w tym specyfikację przyjętych Rozwiązań umieszczono w części OPZ stanowiącą informacje chronione.
- 1.22. Postanowienia 1.3-1.7 oraz część druga OPZ nie mają zastosowania do części pierwszej Przedmiotu Zamówienia, z uwagi na fakt, że podstawowe szkolenie z cyberbezpieczeństwa może być wykonane niezależnie od pozostałych wymagań OPZ.

## **CZĘŚĆ PIERWSZA**

**Szkolenie z zakresu cyberbezpieczeństwa - podstawowe szkolenie budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników IT/OT/ICS**

- 00001 Wykonawca przeprowadzi szkolenie o charakterze podstawowym (świadomościowym) z zakresu cyberbezpieczeństwa i ochrony informacji, ukierunkowane na praktyczne zachowania ograniczające ryzyka adekwatne dla prowadzonej przez Zamawiającego działalności.
- 00002 Program szkolenia musi obejmować zarówno obszar IT, jak i podstawy bezpieczeństwa OT/ICS, w szczególności w zakresie ryzyk procesu, dostępu zdalnego oraz współpracy z dostawcami.
- 00003 Wykonawca dostosuje przykłady i scenariusze do realiów organizacji Zamawiającego (infrastruktura krytyczna/środowisko IT+OT), bez wymagania ujawniania informacji wrażliwych.
- 00004 Wykonawca zapewni, aby szkolenie miało charakter praktyczny i było ukierunkowane na ograniczanie ryzyk związanych z pracą z pocztą elektroniczną, dokumentami, systemami IT i OT oraz komunikacją zewnętrzną.
- 00005 Wykonawca uwzględni w szkoleniu omówienie podstawowych pojęć i odpowiedzialności pracownika, w tym znaczenia poufności, integralności i dostępności informacji w ujęciu praktycznym.
- 00006 Wykonawca omówi w szkoleniu konsekwencje typowych incydentów i błędów użytkowników, w tym skutki finansowe, organizacyjne i prawne.
- 00007 Wykonawca uwzględni w szkoleniu zasady identyfikacji i ochrony informacji wrażliwych w pracy biurowej, w tym danych klientów lub mieszkańców, danych pracowników, dokumentów finansowych, umów i korespondencji.
- 00008 Wykonawca omówi podstawowe zasady ochrony danych osobowych w zakresie niezbędnym dla pracownika biurowego, w tym minimalizację danych i zasadę potrzeby wiedzy.
- 00009 Wykonawca omówi bezpieczne udostępnianie informacji i danych, w tym zasady doboru adresatów, stosowania DW i UDW, ograniczania grona odbiorców oraz weryfikacji właściwego adresata przed wysyłką.

- 00010 Wykonawca omówi bezpieczne przekazywanie plików i dokumentów, w tym stosowanie uprawnień do linków, ograniczeń czasowych, szyfrowania plików oraz przekazywania haseł innym kanałem komunikacji.
- 00011 Wykonawca omówi bezpieczne przechowywanie i przetwarzanie dokumentów, w tym zasady przechowywania na nośnikach i w systemach służbowych oraz ryzyka związane z kopiowaniem na nośniki prywatne.
- 00012 Wykonawca przedstawi możliwości portalu bezpiecznedane.gov.pl oraz havibeenpawne.com w zakresie ustalania wycieku własnych haseł, danych osobistych.
- 00013 Wykonawca przedstawi różnice między http a https.
- 00014 Wykonawca przedstawi zagrożenia hybrydowe dotyczące cyberprzestrzeni, w szczególności zagrożenia dezinformacji, ataków hybrydowych, wykorzystywania kont społecznościowych.
- 00015 Wykonawca przedstawi zagrożenia ochrony sieci WiFi w domu i pracy – bezpieczne hasła, szyfrowanie, konieczność aktualizacji urządzeń sieciowych.
- 00016 Wykonawca przedstawi zagrożenie podatności urządzeń, zarządzania podatnościami, zasad aktualizacji sprzętu i oprogramowania i konsekwencji wynikających z zaniechań aktualizacji bezpieczeństwa.
- 00017 Wykonawca przedstawi zagrożenia wynikające z publikowania danych o infrastrukturze w BIP, zamówieniach publicznych, zdjęć w portalach Internetowych infrastruktury OT.
- 00018 Wykonawca omówi zasady bezpiecznego drukowania i przechowywania wydruków oraz zasady niszczenia dokumentów i utylizacji nośników informacji.
- 00019 Wykonawca uwzględni w szkoleniu rozpoznawanie zagrożeń socjotechnicznych i phishingu w kanałach e-mail, SMS, telefonicznych i komunikatorach.
- 00020 Wykonawca przedstawi zagrożenia wynikające z wykorzystania bezpłatnych rozwiązań chmurowych, mailowych czy modeli językowych AI, które wykorzystują do dalszej analizy dane, które tam przechowujemy – w kontekście zagrożeń utraty prywatności, danych chronionych.



- 00021 Wykonawca przedstawi zagrożenia wynikające z instalacji aplikacji na telefony komórkowe.
- 00022 Wykonawca zaprezentuje metody weryfikacji aplikacji instalowanych na telefonach komórkowych – pod kątem ich uprawnień.
- 00023 Wykonawca przedstawi cechy prób wyłudzeń typu podszywanie się pod osobę publiczną, instytucję lub przełożonego, w tym scenariusze „pilny przelew”, „zmiana numeru rachunku” oraz „pilna prośba przełożonego” wraz z zasadami ich weryfikacji.
- 00024 Wykonawca omówi zasady bezpiecznego postępowania z linkami, załącznikami oraz kodami QR, w tym typowe mechanizmy infekcji i wyłudzeń.
- 00025 Wykonawca omówi wymagania bezpiecznego uwierzytelniania, w tym zasady tworzenia haseł, stosowania menedżerów haseł oraz uwierzytelniania wieloskładnikowego, o ile jest dostępne u Zamawiającego.
- 00026 Wykonawca omówi zasady ochrony kont użytkowników przed przejęciem, w tym rozpoznawanie nietypowych logowań, podejrzanych powiadomień i prób wymuszeń potwierdzeń.
- 00027 Wykonawca omówi zasady bezpiecznego korzystania ze sprzętu służbowego, w tym blokadę ekranu, aktualizacje oraz bezpieczne korzystanie z przeglądarki i aplikacji biurowych w ujęciu użytkownika.
- 00028 Wykonawca omówi ryzyka związane z nośnikami USB i plikami z nieznanych źródeł oraz zasady postępowania ograniczające ryzyko infekcji.
- 00029 Wykonawca uwzględni w szkoleniu zasady bezpiecznej pracy zdalnej i mobilnej, w tym ryzyka WiFi publicznych, hotspotów, pracy na urządzeniach prywatnych oraz zasady ochrony ekranu w miejscach publicznych.
- 00030 Wykonawca omówi podstawowe zasady korzystania z firmowych kanałów dostępu zdalnego, w tym VPN, jeżeli stosowany oraz ryzyka związane z obchodzeniem przyjętych zasad.

- 00031 Wykonawca omówi rozpoznawanie objawów złośliwego oprogramowania i ransomware w ujęciu użytkownika, w tym typowe symptomy oraz podstawowe zasady pierwszych działań.
- 00032 Wykonawca wskaże czynności niedopuszczalne w przypadku podejrzenia incydentu, w tym samodzielne „czyszczenie”, ukrywanie zdarzenia, chaotyczne resetowanie lub przenoszenie danych na prywatne nośniki.
- 00033 Wykonawca omówi minimalne zasady zgłaszania incydentów, w tym co należy zgłaszać, w jakim czasie i jakim kanałem zgodnie z procedurami Zamawiającego lub przyjętym modelem zgłoszeń.
- 00034 Wykonawca wskaże minimalny zestaw informacji, który uczestnik powinien przekazać przy zgłoszeniu incydentu, w tym czas zdarzenia, użyte urządzenie, konto, opis objawów oraz dostępne zrzuty ekranu.
- 00035 Wykonawca uwzględni w programie zasady klasyfikacji i ochrony informacji, w tym informacji wrażliwych z perspektywy IT i OT (np. topologie, konfiguracje, listy adresacji, konta serwisowe, dokumentacja technologiczna).
- 00036 Wykonawca omówi podstawowe obowiązki i dobre praktyki w zakresie ochrony danych osobowych w zakresie niezbędnym dla użytkownika systemów, w tym bezpieczne udostępnianie, przechowywanie oraz przekazywanie informacji.
- 00037 Wykonawca omówi zasady bezpiecznego uwierzytelniania i zarządzania dostępem, w tym: hasła, MFA, menedżer haseł, zasadę najmniejszych uprawnień, rozdzielanie kont uprzywilejowanych od kont użytkownika.
- 00038 Wykonawca omówi ryzyka związane z kontami serwisowymi i współdzielonymi oraz minimalne praktyki ograniczające nadużycia (w tym w środowisku OT/ICS).
- 00039 Wykonawca omówi mechanizmy socjotechniki i phishingu (e-mail, SMS, telefon, komunikatory), w tym rozpoznawanie cech prób wyłudzeń.
- 00040 Wykonawca przedstawi scenariusze typowe dla IT/OT, w szczególności podszywanie się pod dostawcę/serwis oraz presję „pilnej awarii” i żądania zdalnego dostępu, przekazania konfiguracji lub danych uwierzytelniających.

- 00041 Wykonawca przedstawi zasady niezależnej weryfikacji próśb i poleceń (oddzwanianie, drugi kanał, zatwierdzenie przez osobę uprawnioną).
- 00042 Wykonawca omówi różnice IT vs OT/ICS na poziomie podstawowym, w szczególności: priorytet bezpieczeństwa procesu, ograniczenia aktualizacji, długie cykle życia urządzeń, konsekwencje przestoju.
- 00043 Wykonawca omówi typowe ryzyka w OT/ICS, w tym: nieautoryzowana zmiana nastaw/konfiguracji, manipulacja danymi pomiarowymi, utrata widoczności/sterowania, propagacja incydentów z IT do OT.
- 00044 Wykonawca przedstawi minimalne wymagania bezpiecznego zdalnego dostępu do systemów IT i OT/ICS, w tym: konta imienne, MFA, ograniczenie czasowe dostępu, zatwierdzanie dostępu, rejestrowanie zdarzeń/logowanie, ograniczanie uprawnień do niezbędnego zakresu.
- 00045 Wykonawca omówi ryzyka stałych dostępu serwisowych oraz stosowania niezatwierdzonych narzędzi zdalnych i „obejść” procedur (w ujęciu świadomościowym).
- 00046 Wykonawca omówi zasady bezpiecznej współpracy z dostawcami/serwisem w trybie zdalnym i onsite, w tym: weryfikację tożsamości, zasady wprowadzania zmian, ścieżkę zgód, minimalizację uprawnień, odpowiedzialność i rozliczalność.
- 00047 Wykonawca omówi typowe ryzyka związane z presją dostawcy („musi być stały dostęp”, „tylko na chwilę”) oraz zasady eskalacji w przypadku potrzeby niestandardowego dostępu.
- 00048 Wykonawca omówi typowy przebieg incydentu ransomware i jego skutki operacyjne w IT oraz potencjalne oddziaływanie na OT/ICS.
- 00049 Wykonawca wskaże zachowania pracowników, które ograniczają straty (wczesne zgłoszenie, nieukrywanie incydentu, niepodejmowanie niekontrolowanych działań), oraz podstawowe zasady postępowania z nośnikami i plikami w sytuacji podejrzenia incydentu.
- 00050 Wykonawca omówi sygnały ostrzegawcze incydentów w IT oraz w OT/ICS na poziomie podstawowym (np. nietypowe logowania, prośby o ponowne MFA, anomalie trendów/alertów, nieoczekiwane restarty, utrata komunikacji).

- 00051 Wykonawca zapewni elementy praktyczne obejmujące co najmniej trzy ćwiczenia z udziałem uczestników: identyfikację phishingu, analizę ryzyk w wiadomości (link/załącznik/QR) oraz scenariusz weryfikacji „pilnej prośby” dotyczącej płatności lub danych.
- 00052 Wykonawca zapewni materiały szkoleniowe dla każdego uczestnika obejmujące co najmniej checklistę podstawowych zasad bezpiecznej pracy, listę „czerwonych flag” dla prób wyłudzeń oraz instrukcję zgłaszania incydentów.
- 00053 Wykonawca przeprowadzi po szkoleniu krótką weryfikację wiedzy w formie testu lub quizu sytuacyjnego.
- 00054 Wykonawca przekaze Zamawiającemu zbiorcze podsumowanie wyników weryfikacji wiedzy oraz obszarów wymagających wzmocnienia, bez identyfikacji uczestników.
- 00055 Szkoleniem objętych zostanie łącznie 10 pracowników Zamawiającego, w tym 1 administrator systemów IT.
- 00056 Szkolenie będzie realizowane stacjonarnie w siedzibie Zamawiającego.
- 00057 Czas trwania szkolenia dla każdej grupy nie może być krótszy niż 8 godzin dydaktycznych, realizowanych w jednym dniu lub w uzgodnionym harmonogramie.
- 00058 Szkolenie musi być prowadzone w języku polskim.
- 00059 Po zakończeniu szkolenia Wykonawca przekaze Zamawiającemu dokumentację potwierdzającą realizację szkolenia (np. lista obecności, agenda, certyfikaty).
- 00060 Szkolenie musi być zgodne z obowiązującymi przepisami prawa, w szczególności RODO, KRI, ustawą o krajowym systemie cyberbezpieczeństwa oraz dobrymi praktykami cyberbezpieczeństwa oraz najnowszym stanem wiedzy technicznej.