

OPIS PRZEDMIOTU ZAMÓWIENIA

w postępowaniu prowadzonym w trybie otwartej procedury konkurencyjnej pn.
**„Wdrożenie kompleksowych rozwiązań w zakresie cyberbezpieczeństwa
dla Przedsiębiorstwa Komunalnego w Tucholi Sp. z o.o.,
w ramach projektu „Cyberbezpieczne Wodociągi”**

CZĘŚĆ I – REALIZACJA ZADAŃ ORGANIZACYJNYCH I KOMPETENCYJNYCH

1. Przedmiotem niniejszego postępowania jest wdrożenie kompleksowych rozwiązań w zakresie cyberbezpieczeństwa dla Przedsiębiorstwa Komunalnego w Tucholi Sp. z o.o., w ramach projektu „Cyberbezpieczne Wodociągi, poprzez realizację zadań organizacyjnych i kompetencyjnych (część I zamówienia).
2. Zakres rzeczowy poszczególnych części określono szczegółowo w dalszej części OPZ. Realizacja zamówienia ma zapewnić osiągnięcie przez Zamawiającego celów i wskaźników określonych we wniosku o objęcie przedsięwzięcia wsparciem oraz dostosowanie do wymagań wynikających z przepisów o krajowym systemie cyberbezpieczeństwa.

PRZEPROWADZENIE SZCZEGÓŁOWEJ ANALIZY PRZEDWDROŻENIOWEJ

Przed przystąpieniem do opracowania lub aktualizacji dokumentacji SZBI, SZCD, BCP i DRP Wykonawca zobowiązany jest przeprowadzić szczegółową analizę przedwdrożeniową w siedzibie i obiektach Zamawiającego.

Celem analizy jest rzeczywiste rozpoznanie organizacji Zamawiającego, realizowanych procesów, obiegu informacji i dokumentów, wykorzystywanych systemów IT i OT, infrastruktury technicznej, istniejących zabezpieczeń oraz zależności pomiędzy procesami organizacyjnymi i systemami teleinformatycznymi.

Analiza przedwdrożeniowa nie może zostać przeprowadzona wyłącznie na podstawie ankiet, formularzy przesłanych Zamawiającemu lub konsultacji zdalnych.

1. Wymagania ogólne

Zamawiający wymaga przeprowadzenia przez Wykonawcę **analizy przedwdrożeniowej**, obejmującej zapoznanie się z organizacją pracy Zamawiającego, funkcjonującym obiegiem dokumentów, stosowanymi procedurami, wykorzystywanymi systemami i rozwiązaniami organizacyjno-technicznymi oraz innymi uwarunkowaniami mającymi wpływ na prawidłową realizację przedmiotu zamówienia.

Analiza przedwdrożeniowa powinna zostać przeprowadzona **w zakresie i wymiarze niezbędnym do prawidłowego rozpoznania potrzeb Zamawiającego oraz przygotowania i realizacji przedmiotu zamówienia.**

Wykonawca zobowiązany jest zapewnić udział osób posiadających wiedzę i doświadczenie odpowiednie do zakresu prowadzonej analizy oraz uzgodnić z Zamawiającym sposób i termin jej przeprowadzenia.

Rezultatem analizy będzie przedstawienie Zamawiającemu wniosków oraz rekomendacji dotyczących sposobu realizacji przedmiotu zamówienia, z uwzględnieniem stanu istniejącego oraz zidentyfikowanych potrzeb i uwarunkowań Zamawiającego.

2. Zakres analizy przedwdrożeniowej

W ramach analizy Wykonawca zobowiązany jest co najmniej do:

1. przeprowadzenia spotkania otwierającego z przedstawicielami Zamawiającego;
2. zapoznania się ze strukturą organizacyjną Zamawiającego oraz zakresem odpowiedzialności poszczególnych komórek i stanowisk;
3. przeprowadzenia wywiadów z osobami odpowiedzialnymi za kluczowe procesy organizacyjne;
4. przeprowadzenia wywiadów z osobami odpowiedzialnymi za IT, OT, bezpieczeństwo informacji, ochronę danych osobowych oraz ciągłość działania – jeżeli takie funkcje zostały wyodrębnione;
5. dokonania analizy rzeczywistego **obiegu dokumentów i informacji**, obejmującej dokumentację papierową i elektroniczną;
6. identyfikacji miejsc powstawania, przetwarzania, przekazywania, przechowywania i archiwizowania informacji;
7. identyfikacji wykorzystywanych systemów informatycznych, aplikacji, baz danych i usług;
8. analizy środowiska IT i OT oraz wzajemnych zależności pomiędzy systemami;
9. identyfikacji aktywów informacyjnych i technicznych mających znaczenie dla bezpieczeństwa informacji i ciągłości działania;
10. analizy sposobu zarządzania kontami, uprawnieniami i dostępem do informacji;
11. analizy stosowanych mechanizmów uwierzytelniania i kontroli dostępu;
12. analizy organizacji wykonywania, przechowywania i odtwarzania kopii zapasowych;
13. analizy istniejących mechanizmów monitorowania, rejestrowania i reagowania na incydenty;
14. analizy stosowanych zabezpieczeń sieciowych, systemowych, organizacyjnych i fizycznych;
15. analizy procesu aktualizacji systemów oraz zarządzania podatnościami;
16. identyfikacji dostawców zewnętrznych oraz zależności od usług świadczonych przez podmioty trzecie;
17. identyfikacji procesów krytycznych Zamawiającego;
18. identyfikacji zależności procesów krytycznych od infrastruktury, systemów IT/OT, personelu, informacji, dostawców i innych zasobów;
19. zebrania danych niezbędnych do przeprowadzenia analizy wpływu na działalność (BIA);
20. zebrania danych niezbędnych do określenia parametrów RTO i RPO;
21. identyfikacji zagrożeń i podatności oraz przeprowadzenia analizy ryzyka;
22. analizy istniejącej dokumentacji SZBI, bezpieczeństwa informacji, ochrony danych, ciągłości działania, procedur awaryjnych i instrukcji eksploatacyjnych;
23. przeprowadzenia wizji infrastruktury i pomieszczeń mających znaczenie dla bezpieczeństwa informacji lub ciągłości działania;
24. przeprowadzenia spotkania podsumowującego wyniki analizy z przedstawicielami Zamawiającego.

3. Wywiady z pracownikami

W ramach analizy Wykonawca zobowiązany jest przeprowadzić bezpośrednie wywiady lub warsztaty z przedstawicielami komórek organizacyjnych i osobami odpowiedzialnymi za procesy objęte analizą.

Wywiady mają służyć w szczególności ustaleniu:

- rzeczywistego przebiegu procesów,
- sposobu obiegu dokumentów i informacji,
- wykorzystywanych systemów i zasobów,
- odpowiedzialności poszczególnych osób,
- zależności pomiędzy procesami,
- sposobu postępowania w przypadku awarii lub niedostępności systemów,
- występujących zagrożeń i problemów,
- istniejących mechanizmów kontrolnych i zabezpieczeń.

Zamawiający wymaga, aby analiza nie ograniczała się wyłącznie do informacji przekazanych przez personel IT.

4. Dokumentowanie realizacji analizy przedwdrożeniowej

Wykonawca zobowiązany jest przeprowadzić analizę przedwdrożeniową **bezpośrednio w siedzibie Zamawiającego**, w zakresie niezbędnym do prawidłowego rozpoznania organizacji pracy, procesów, obiegu dokumentów, stosowanych procedur oraz pozostałych uwarunkowań mających wpływ na realizację przedmiotu zamówienia.

Wykonawca zobowiązany jest prowadzić **dokumentację realizacji analizy przedwdrożeniowej**, umożliwiającą potwierdzenie zakresu faktycznie przeprowadzonych czynności.

Dokumentacja powinna zawierać co najmniej:

1. datę przeprowadzenia czynności,
2. miejsce realizacji czynności,
3. imię i nazwisko konsultanta lub konsultantów uczestniczących w realizacji analizy,
4. opis zakresu wykonanych czynności,
5. wskazanie komórki organizacyjnej, procesu lub obszaru objętego analizą,
6. wskazanie osób lub funkcji uczestniczących w spotkaniach, konsultacjach lub wywiadach – jeżeli dotyczy,
7. najważniejsze ustalenia i wnioski wynikające z przeprowadzonych czynności.

Dokumentacja realizacji analizy przedwdrożeniowej podlega zatwierdzeniu przez przedstawiciela Zamawiającego.

Wykonawca zobowiązany jest zapewnić taki zakres czynności realizowanych w siedzibie Zamawiającego, jaki jest niezbędny do rzetelnego przeprowadzenia analizy oraz prawidłowej realizacji przedmiotu zamówienia.

5. Raport z analizy przedwdrożeniowej

Po zakończeniu analizy Wykonawca przedstawi Zamawiającemu raport z analizy przedwdrożeniowej.

Raport powinien zawierać co najmniej:

1. opis zastosowanej metodyki;
2. opis organizacji i jej kontekstu;
3. opis zidentyfikowanych procesów;
4. opis obiegu informacji i dokumentów;
5. wykaz kluczowych aktywów informacyjnych;
6. charakterystykę środowiska IT i OT;
7. identyfikację procesów krytycznych;
8. identyfikację zależności pomiędzy procesami, systemami, personelem, infrastrukturą i dostawcami;
9. wyniki analizy istniejących zabezpieczeń;
10. zidentyfikowane zagrożenia, podatności i ryzyka;
11. wykaz stwierdzonych niezgodności, braków lub obszarów wymagających poprawy;
12. rekomendacje stanowiące podstawę do opracowania lub aktualizacji SZBI, SZCD, BCP i DRP.

Raport podlega przedstawieniu i omówieniu z Zamawiającym. Zamawiający może zgłosić uwagi do raportu. Wykonawca zobowiązany jest uwzględnić uzasadnione uwagi i przedstawić jego wersję ostateczną.

6. Wymagania dotyczące opracowania dokumentacji

Dokumentacja opracowana w ramach zamówienia musi być indywidualnie dostosowana do rzeczywistej struktury organizacyjnej, procesów, obiegu informacji, infrastruktury oraz środowiska IT i OT Zamawiającego.

Zamawiający nie dopuszcza wykonania przedmiotu zamówienia poprzez przekazanie dokumentacji wzorcowej lub szablonowej, która nie została dostosowana do wyników przeprowadzonej analizy przedwdrożeniowej.

Wyniki analizy przedwdrożeniowej muszą stanowić podstawę opracowania dokumentacji SZBI, analizy ryzyka, SZCD, BIA, BCP i DRP.

OBSZAR ORGANIZACYJNY

Zamawiający wymaga w tym obszarze wykonania następujących zadań: opracowania, aktualizacji i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) wraz z analizą ryzyka oraz opracowaniem i wdrożeniem planów ciągłości działania (BCP) i odtwarzania po awarii (DRP).

Zadanie 1: Przegląd, opracowanie i dostosowanie do nowych wymagań oraz wdrożenie dokumentacji SZBI.

W ramach realizacji zadania Wykonawca opracuje, dostosuje i wdroży dokumentację SZBI, obejmującą w szczególności:

- **Politykę Bezpieczeństwa Informacji (PBI)** – zasady ogólne, zakres SZBI, role i odpowiedzialności, zasady zarządzania ryzykiem i incydentami, audyty, ochronę informacji i danych oraz zasady doskonalenia SZBI,
- **Bezpieczeństwo osobowe** – zasady dotyczące zatrudniania, upoważnień, szkoleń, zmiany zatrudnienia oraz jego zakończenia,
- **Bezpieczeństwo teleinformatyczne** – zasady dotyczące kont i uprawnień, uwierzytelniania, w tym MFA, sprzętu i oprogramowania, poczty elektronicznej, Internetu, ochrony przed szkodliwym oprogramowaniem, dostępu zdalnego, kopii bezpieczeństwa, ochrony sieci, zarządzania podatnościami, rejestrowania i monitorowania zdarzeń, zarządzania zmianą i aktualizacjami bezpieczeństwa oraz współpracy z dostawcami i serwisem,
- **Bezpieczeństwo fizyczne** – zasady dotyczące kontroli dostępu, obszarów bezpiecznych, ochrony fizycznej, kluczy, kodów alarmowych i ewidencji dostępu,
- **Zarządzanie aktywami informacyjnymi** – zasady identyfikacji i ewidencji aktywów, określania właścicieli zasobów oraz wycofywania aktywów,
- **Klasyfikacja i postępowania z informacjami** – zasady klasyfikowania, oznaczania, przechowywania, udostępniania i bezpiecznego obiegu informacji,
- **Zarządzanie ryzykiem** – zasady identyfikacji, szacowania i oceny ryzyka, postępowania z ryzykiem oraz prowadzenia rejestru ryzyk,
- **Zarządzanie incydentami bezpieczeństwa informacji** – zasady zgłaszania, rejestrowania, klasyfikacji, obsługi i dokumentowania incydentów oraz ich raportowania zgodnie z obowiązującymi przepisami,
- dostosowanie opracowanej dokumentacji SZBI do zakresu działalności Zamawiającego oraz wykorzystywanych systemów IT i OT,
- wdrożenie opracowanej dokumentacji poprzez jej przedstawienie i omówienie z osobami odpowiedzialnymi za realizację zadań związanych z bezpieczeństwem informacji.

Dokumentacja SZBI musi być zgodna z obowiązującymi przepisami prawa, w szczególności:

- 1) ustawą o krajowym systemie cyberbezpieczeństwa (KSC),
- 2) przepisami RODO,
- 3) Krajowymi Ramami Interoperacyjności (KRI) – w zakresie mającym zastosowanie,
- 4) z uwzględnieniem wytycznych normy PN-EN ISO/IEC 27001).

W ramach realizacji zadania Wykonawca na podstawie wyników analizy przedwdrożeniowej opracuje dokumentację SZBI dostosowaną do faktycznie występujących ryzyk i procesów, uwzględniając specyfikę działania jednostki. Struktura SZBI powinna mieć charakter hierarchiczny (tj. opisywać bezpieczeństwo informacji na różnych poziomach szczegółowości) i obejmować co najmniej następujące dokumenty:

- 1) Polityka Bezpieczeństwa Informacji,
- 2) Deklaracja Stosowania,
- 3) Bezpieczeństwo Fizyczne i Środowiskowe,
- 4) Zarządzanie Ciągłością Działania,
- 5) Instrukcja zarządzania systemem informatycznym,
- 6) Zarządzanie ryzykiem,
- 7) Audyty wewnętrzne SZBI,
- 8) Przegląd zarządzania,
- 9) Zarządzanie udokumentowaną informacją,
- 10) Działania korygujące,

- 11) Klasyfikacja informacji,
- 12) Bezpieczeństwo zasobów ludzkich,
- 13) Zarządzanie incydentami bezpieczeństwa,
- 14) Zarządzania relacjami z dostawcami.

Zamawiający wymaga, aby dokumentacja w swoim zakresie obejmowała przynajmniej następujące zagadnienia:

- 1) organizacja i odpowiedzialności w zakresie bezpieczeństwa informacji,
- 2) kontekst organizacji,
- 3) cele SZBI,
- 4) komunikacja wewnętrzna i zewnętrzna,
- 5) identyfikacja aktywów informacyjnych i klasyfikacji informacji przetwarzanych u Zamawiającego,
- 6) metodyka szacowania ryzyka oraz postępowanie z ryzykiem związanym z utratą poufności, integralności i dostępności informacji przetwarzanych u Zamawiającego,
- 7) bezpieczeństwo w procesach zarządzania zasobami ludzkimi,
- 8) szkolenia z zakresu bezpieczeństwa informacji,
- 9) kontrola dostępu,
- 10) bezpieczeństwo fizyczne i środowiskowe,
- 11) dostęp do pomieszczeń i obszarów szczególnie chronionych,
- 12) klasyfikacja informacji,
- 13) odpowiedzialność za zasoby,
- 14) postępowanie z nośnikami informacji,
- 15) użytkowanie urządzeń mobilnych i praca zdalna,
- 16) zarządzanie sprzętem informatycznym,
- 17) instalacja oprogramowania,
- 18) ochrona przed oprogramowaniem złośliwym,
- 19) kopie zapasowe,
- 20) zarządzanie zmianami, w szczególności w systemach informatycznych oraz infrastrukturze informatycznej,
- 21) zarządzanie dokumentacją infrastruktury informatycznej,
- 22) monitorowanie systemów informatycznych,
- 23) zarządzanie pojemnością systemów,
- 24) serwis i konserwacja infrastruktury informatycznej,
- 25) zarządzanie podatnościami technicznymi,
- 26) zarządzanie incydentami bezpieczeństwa,
- 27) zabezpieczenia kryptograficzne,
- 28) bezpieczeństwo sieci i transmisji danych,
- 29) ochrona własności intelektualnej,
- 30) bezpieczeństwo informacji w relacjach z dostawcami,
- 31) zasady bezpieczeństwa informacji w procesach pozyskiwania, rozwoju i utrzymania systemów informacyjnych,
- 32) weryfikacja zgodności z wymaganiami prawnymi,
- 33) korzystanie z poczty elektronicznej i Internetu,
- 34) zarządzanie usługami informatycznymi,
- 35) utrzymanie i doskonalenie SZBI,
- 36) przeprowadzanie audytów SZBI.

Dokumentacja zostanie przekazana Zamawiającemu w formie edytowalnych plików elektronicznych:

- 1) w przypadku polityk, procedur i instrukcji w formacie .docx
- 2) w przypadku ewidencji, rejestrów i zestawień w formacie .docx lub .xlsx

Zadanie 2: Opracowanie i wdrożenie Systemu Zarządzania Ciągłością Działania (SZCD) dla procesów krytycznych oraz systemów IT/OT.

W ramach tego zadania Wykonawca opracuje i wdroży System Zarządzania Ciągłością Działania (SZCD) zgodny co najmniej z wymaganiami normy PN-EN ISO 22301. W ramach realizacji zadania Wykonawca:

- określi kontekst działania organizacji i zakres SZCD,
- zidentyfikuje procesy krytyczne oraz niezbędne zasoby,
- przeprowadzi Analizę Wpływu Biznesowego (BIA),
- określi parametry ciągłości działania, w szczególności RTO i RPO,
- przeprowadzi analizę ryzyka i określi sposoby postępowania z ryzykiem,
- opracuje strategie i rozwiązania zapewnienia ciągłości działania,
- określi role i odpowiedzialności oraz zasady komunikacji,
- opracuje i wdroży dokumentację SZCD, w tym zasady ćwiczeń i testowania, audytu, przeglądu zarządzania oraz ciągłego doskonalenia,
- przeprowadzi instruktaż lub warsztaty dla wyznaczonego personelu.

Zakres prac obejmuje w szczególności:

Analiza stanu obecnego

- 1) identyfikacja procesów krytycznych Zamawiającego,
- 2) przeprowadzenie analizy wpływu na działalność (BIA),
- 3) przeprowadzenie analizy ryzyka w obszarze ciągłości działania STI (IT i OT),
- 4) ocena istniejących zabezpieczeń organizacyjnych, technicznych i proceduralnych.

Opracowanie Systemu Zarządzania Ciągłością Działania (SZCD)

Wykonawca opracuje i udokumentuje SZCD obejmujący co najmniej:

- 1) politykę ciągłości działania,
- 2) strukturę organizacyjną SZCD (role, odpowiedzialności, zespoły),
- 3) procedury zarządzania incydentami i kryzysami,
- 4) procedury utrzymania, testowania, przeglądów i doskonalenia SZCD,
- 5) wskaźniki efektywności SZCD (KPI),
- 6) zasady monitorowania ryzyk i aktualizacji dokumentacji.

Wdrożenie SZCD

- 1) przygotowanie pełnej dokumentacji SZCD w formie edytowalnej,
- 2) przeprowadzenie warsztatów i konsultacji z personelem Zamawiającego,
- 3) wsparcie we wdrożeniu struktur, ról i procedur,
- 4) rekomendacje dotyczące dalszego doskonalenia systemu.

Wymagania dodatkowe

SZCD musi:

- 5) obejmować systemy IT i OT, infrastrukturę techniczną, zasoby informacyjne i zależności organizacyjne,
- 6) wspierać spełnienie wymagań prawnych, w tym RODO, KRI, NIS2, ustawy o krajowym systemie cyberbezpieczeństwa,
- 7) uwzględniać analizę ryzyk związanych z przerwami w działaniu systemów teleinformatycznych,
- 8) uwzględniać scenariusze awarii technicznych, cyberataków, zdarzeń losowych oraz niedostępności personelu.

Dokumentacja zostanie przekazana Zamawiającemu w formie edytowalnych plików elektronicznych:

- 1) w przypadku polityk, procedur i instrukcji w formacie .docx
- 2) w przypadku ewidencji, rejestrów i zestawień w formacie .docx lub .xlsx

Zadanie 3. Opracowanie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP).

W ramach realizacji zadania Wykonawca opracuje kompletne Plany Ciągłości Działania (BCP) oraz Plany Odtwarzania po Awarii (DRP) dla zidentyfikowanych procesów krytycznych systemów IT i OT.

W ramach realizacji zadania Wykonawca opracuje plany ciągłości działania dla procesów krytycznych, z uwzględnieniem wyników BIA, analizy ryzyka oraz przyjętych rozwiązań ciągłości działania.

Plan ciągłości działania (BCP)

W ramach realizacji zadania Wykonawca opracuje plany ciągłości działania dla procesów krytycznych, z uwzględnieniem wyników BIA, analizy ryzyka oraz przyjętych rozwiązań ciągłości działania. Plany powinny uwzględniać w szczególności:

- scenariusze awaryjne związane z działalnością Zamawiającego, w tym systemami IT/OT,
- działania awaryjne i procedury zastępcze,
- role i odpowiedzialności,
- zasady komunikacji i kontakty kryzysowe,
- niezbędne zasoby,
- zasady powrotu do normalnego funkcjonowania,
- zasady ćwiczeń, testowania, aktualizacji i raportowania.

Plan odtwarzania po awarii (DRP)

W ramach realizacji zadania Wykonawca opracuje plan odtwarzania po awarii dla kluczowych systemów i zasobów IT/OT, z uwzględnieniem ich wzajemnych zależności, wymaganych parametrów RTO/RPO oraz dostępnych kopii zapasowych. DRP powinien określać podstawowe zasady odtwarzania systemów, danych i urządzeń oraz weryfikacji poprawności ich odtworzenia. Plany powinny uwzględniać w szczególności:

- procedury odtworzenia systemów, aplikacji i danych,
- identyfikację zależności pomiędzy systemami,

- wymagania infrastrukturalne i organizacyjne,
- zasady wykonywania, przechowywania i odtwarzania kopii zapasowych,
- testy odtwarzania oraz kryteria ich oceny,
- procedury odtwarzania zgodne z określonymi RTO i RPO.

Wymagania dodatkowe

Plany BCP i DRP muszą:

- 1) zapewniać zdolność organizacji do utrzymania lub szybkiego przywrócenia kluczowych funkcji i systemów IT/OT,
- 2) być zgodne z normami i dobrymi praktykami w zakresie ciągłości działania i bezpieczeństwa informacji,
- 3) uwzględniać różne scenariusze awarii, w tym cyberataki, awarie techniczne, zdarzenia losowe i niedostępność personelu,
- 4) jednoznacznie określać role, odpowiedzialności i strukturę zespołów odpowiedzialnych za realizację planów,
- 5) uwzględniać dostępność zasobów technicznych, ludzkich i organizacyjnych niezbędnych do realizacji planów.

W ramach zadania Wykonawca przeprowadzi co najmniej jedno uzgodnione z Zamawiającym ćwiczenie lub test BCP/DRP oraz sporządzi krótkie podsumowanie wyników.

Dokumentacja zostanie przekazana Zamawiającemu w formie edytowalnych plików elektronicznych:

- 1) w przypadku polityk, procedur i instrukcji w formacie .docx
- 2) w przypadku ewidencji, rejestrów i zestawień w formacie .docx lub .xlsx

OBSZAR KOMPETENCYJNY

Zamawiający wymaga w tym obszarze wykonania następujących zadań:

1. Zadanie 1: Podstawowe szkolenie stacjonarne dla pracowników budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników IT/OT/ICT,
2. Zadanie 2: Szkolenia z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji,
3. Zadanie 3: Szkolenia - testy symulacyjne z zakresu cyberbezpieczeństwa,
4. Zadanie 4: Szkolenia specjalistyczne dla informatyka w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa,
5. Zadanie 5: Szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcje personelu, w szczególności sposób postępowania specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami.

Zadanie 1. Podstawowe szkolenie stacjonarne dla pracowników budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników IT/OT/ICT.

Zakres szkolenia:

- 1) Bezpieczeństwo informacji w polskim prawie.

- 2) Socjotechniki, przykłady zastosowania.
- 3) Przykłady aktualnych ataków, w tym kampanii socjotechnicznych.
- 4) Kradzieże i wyłudzenia informacji.
- 5) Możliwe skutki udanego cyberataku – omówienie i przykłady.
- 6) Kultura ochrony informacji, dojrzałość organizacji.
- 7) Metody codziennej ochrony informacji – bezpieczna praca w systemach informatycznych, bezpieczeństwo fizyczne miejsca pracy, aspekty organizacyjne.
- 8) Cyberbezpieczeństwo w pracy zdalnej – dobre praktyki i wskazówki.
- 9) Szyfrowanie dokumentów w ramach dostępnych funkcji w pakiecie Office.
- 10) Szyfrowanie dowolnego pliku programem zewnętrznym.
- 11) Bezpieczeństwo urządzeń mobilnych.
- 12) Fake news – identyfikacja i walka z fałszywymi wiadomościami.
- 13) Zagrożenia związane z narzędziami sztucznej inteligencji (AI).
- 14) OSINT (biały wywiad) – przykłady i zastosowanie w wodociągach.
- 15) Sesja pytań i odpowiedzi.

Organizacja szkolenia:

1. Szkolenie zostanie przeprowadzone **w trybie stacjonarnym, w siedzibie Zamawiającego.**
2. Szkoleniem zostanie objętych około **32 pracowników Zamawiającego.**
3. Szkolenie zostanie przeprowadzone w ramach **3 edycji**, przy czym każda edycja będzie przeznaczona dla grupy liczącej około **10 uczestników.**
4. Każda edycja szkolenia będzie obejmowała ten sam zakres tematyczny.
5. Czas trwania jednej edycji szkolenia wynosi **6 godzin zegarowych**, z uwzględnieniem czasu przeznaczonego na omówienie zagadnień praktycznych, przykładów oraz sesję pytań i odpowiedzi.
6. Łączny wymiar realizacji szkolenia wynosi **18 godzin zegarowych** (3 edycje × 6 godzin).
7. Zamawiający dokona podziału pracowników na poszczególne grupy. Wykonawca przeprowadzi poszczególne edycje w terminach uzgodnionych z Zamawiającym.
8. Wykonawca zapewni każdemu uczestnikowi możliwość aktywnego udziału w szkoleniu, zadawania pytań oraz konsultacji zagadnień związanych z tematyką szkolenia.
9. Szkolenie musi być prowadzone w języku polskim.
10. Możliwość dopuszczenia szkolenia online dla osób nieobecnych.

Zadanie 2. Szkolenia z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji.

Zakres szkolenia:

1. Podstawy cyberbezpieczeństwa (podstawowe pojęcia i zasady działania).
2. Cyberbezpieczeństwo w sektorze wodno-kanalizacyjnym w kontekście bezpieczeństwa państwa.
3. Przegląd aktualnych zagrożeń i trendów w cyberprzestrzeni.
4. Analiza wybranych przepisów rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów

publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773) i ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2026 poz. 20 ze zm.; dalej: UoKSC).

5. Omówienie głównych zasad Systemu Zarządzania Bezpieczeństwem Informacji, podziału odpowiedzialności i zakresu obowiązków.
6. Tworzenie i implementacja polityk, procedur i innych udokumentowanych informacji.
7. Monitorowanie, przeglądy i doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji.
8. Metody identyfikacji zagrożeń i oceny ryzyka.
9. Procesy i procedury zarządzania incydentami oraz role poszczególnych pracowników.
10. Incydenty w kontekście zachowania ciągłości działania w sektorze wodno-kanalizacyjnym.
11. Rola kadry kierowniczej w zakresie cyberbezpieczeństwa i ciągłości działania.
12. Zasady postępowania w razie wprowadzenia stopni alarmowych CRP dotyczących zagrożeń w cyberprzestrzeni.
13. Przywództwo, motywowanie zespołu i promowanie kultury bezpieczeństwa.

Organizacja szkolenia:

1. Szkolenie zostanie przeprowadzone w trybie **stacjonarnym, w siedzibie Zamawiającego**.
2. Szkoleniem zostanie objętych około **12 osób**.
3. W celu zapewnienia **ciągłości funkcjonowania Zamawiającego oraz możliwości wykonywania bieżących obowiązków służbowych**, szkolenie zostanie przeprowadzone w ramach **2 odrębnych edycji**, dla grup liczących około **6 osób każda**.
4. Każda z grup zostanie objęta **pełnym i jednakowym zakresem tematycznym szkolenia** określonym przez Zamawiającego.
5. Czas trwania jednej edycji szkolenia wynosi **6 godzin zegarowych**. Łączny wymiar realizacji szkolenia wynosi **12 godzin zegarowych** (2 edycje × 6 godzin).
6. Podział uczestników na poszczególne grupy zostanie dokonany przez Zamawiającego z uwzględnieniem organizacji pracy oraz konieczności zapewnienia ciągłości działania poszczególnych komórek organizacyjnych.
7. Terminy przeprowadzenia poszczególnych edycji zostaną uzgodnione z Zamawiającym. Zamawiający dopuszcza przeprowadzenie obu edycji w różnych dniach.
8. Szkolenie powinno mieć charakter praktyczny i uwzględniać przykłady zagrożeń oraz incydentów odnoszących się, w miarę możliwości, do specyfiki działalności Zamawiającego, w szczególności środowiska IT/OT/ICT oraz infrastruktury wodociągowo-kanalizacyjnej.
9. Wykonawca zapewni uczestnikom możliwość aktywnego udziału w szkoleniu, zadawania pytań oraz konsultowania zagadnień związanych z jego tematyką.

Zadanie 3: Szkolenia - testy symulacyjne z zakresu cyberbezpieczeństwa.

Organizacja szkolenia:

1. Szkolenie zostanie przeprowadzone w trybie **stacjonarnym, w siedzibie Zamawiającego**.
2. Szkoleniem zostaną objęci **wszyscy pracownicy Zamawiającego – około 44 osoby**.

3. W celu zapewnienia **ciągłości funkcjonowania Zamawiającego oraz możliwości wykonywania bieżących obowiązków służbowych**, szkolenie zostanie przeprowadzone w ramach **4 odrębnych edycji**, dla grup liczących około **11 osób każda**.
4. Każda z grup zostanie objęta **pełnym i jednakowym zakresem szkolenia oraz testów symulacyjnych**.
5. Czas trwania jednej edycji szkolenia wynosi **minimum 3 godziny zegarowe**, łącznie z przerwami. Łączny minimalny wymiar realizacji szkolenia wynosi **12 godzin zegarowych** (4 edycje × minimum 3 godziny).
6. Podział pracowników na poszczególne grupy zostanie dokonany przez Zamawiającego, z uwzględnieniem struktury organizacyjnej, zakresu obowiązków pracowników oraz konieczności zapewnienia **ciągłości działania poszczególnych komórek organizacyjnych i procesów realizowanych przez Zamawiającego**.
7. Terminy przeprowadzenia poszczególnych edycji zostaną uzgodnione z Zamawiającym. Zamawiający dopuszcza przeprowadzenie poszczególnych edycji w różnych dniach.
8. Szkolenie oraz testy symulacyjne muszą być prowadzone **w języku polskim**.
9. W przypadku nieobecności pracownika podczas wyznaczonej edycji szkolenia Zamawiający dopuszcza możliwość przeprowadzenia dla takiej osoby **szkolenia uzupełniającego w formie zdalnej (online)**, o ile charakter danego testu lub ćwiczenia umożliwia jego prawidłową realizację w tej formie.
10. Testy symulacyjne powinny mieć **charakter praktyczny** i uwzględniać scenariusze zagrożeń możliwych do wystąpienia w środowisku Zamawiającego.
11. Po przeprowadzeniu testów Wykonawca zobowiązany jest do omówienia z uczestnikami zastosowanych scenariuszy, prawidłowych i nieprawidłowych sposobów reakcji oraz zasad właściwego postępowania w przypadku wystąpienia danego rodzaju zagrożenia.

Zadanie 4. Szkolenia specjalistyczne dla informatyka w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa.

1. Szkolenie zostanie przeprowadzone w trybie **stacjonarnym, w siedzibie Zamawiającego**.
2. Szkolenie przeznaczane jest dla pracownika lub pracowników odpowiedzialnych za administrację i utrzymanie środowiska informatycznego Zamawiającego. W szkoleniu udział będzie brało około **2 pracowników**.
3. Szkolenie zostanie przeprowadzone w ramach **1 edycji**.
4. Czas trwania szkolenia wynosi **minimum 6 godzin zegarowych**, łącznie z przerwami.
5. Szkolenie musi być prowadzone **w języku polskim** przez osobę posiadającą wiedzę i doświadczenie techniczne w zakresie rozwiązań i środków bezpieczeństwa objętych szkoleniem.
6. Szkolenie powinno mieć **charakter techniczny i praktyczny** oraz odnosić się bezpośrednio do środowiska informatycznego Zamawiającego, w szczególności do zastosowanych lub planowanych do zastosowania w ramach realizacji projektu środków bezpieczeństwa.
7. Zakres szkolenia powinien obejmować co najmniej konfigurację, administrację, monitorowanie, utrzymanie, aktualizację oraz diagnostykę zastosowanych rozwiązań bezpieczeństwa, a także zasady reagowania na wykryte zagrożenia, zdarzenia i incydenty.
8. W ramach szkolenia Wykonawca powinien przedstawić zasady prawidłowej eksploatacji zastosowanych rozwiązań, wykonywania podstawowych czynności administracyjnych, analizy alertów i logów, wykonywania kopii konfiguracji oraz odtwarzania konfiguracji – w zakresie właściwym dla zastosowanych rozwiązań.

9. Wykonawca zobowiązany jest umożliwić uczestnikom wykonywanie czynności praktycznych oraz konsultowanie konfiguracji i sposobu funkcjonowania zastosowanych lub planowanych do zastosowania środków bezpieczeństwa.
10. W przypadku nieobecności uczestnika w uzgodnionym terminie Zamawiający dopuszcza możliwość przeprowadzenia szkolenia **w formie zdalnej (online)**, pod warunkiem zapewnienia możliwości realizacji pełnego zakresu szkolenia, w tym części praktycznej.
11. Termin szkolenia zostanie uzgodniony z Zamawiającym i powinien zostać skoordynowany z wdrożeniem poszczególnych środków bezpieczeństwa w sposób umożliwiający przeprowadzenie szkolenia na rozwiązaniach zastosowanych lub skonfigurowanych dla Zamawiającego.

Zadanie 5. Szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcje personelu, w szczególności sposób postępowania specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami.

Szkolenia dla pracowników połączone z testami socjotechnicznymi swoim zakresem powinny obejmować:

1. Cele Systemu Zarządzania Bezpieczeństwem Informacji, jego aspekty praktyczne, rola i odpowiedzialność poszczególnych pracowników.
2. Rozpoznawanie zagrożeń, w tym rodzaje ataków, ransomware i malware, phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu Business E-mail Compromise oraz techniki stosowane w atakach socjotechnicznych, takie jak pretexting, baiting, vishing, atak telefoniczny, spoofing, atak odwrócony – zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa.
3. Wpływ zagrożeń na działalność wod.-kan., w tym konsekwencje ataków cybernetycznych, ryzyka utraty danych, naruszenia bezpieczeństwa informacji oraz szkód reputacyjnych.
4. Ochrona danych i informacji, w tym środki ochrony, takie jak silne hasła, uwierzytelnianie wieloskładnikowe, klucze sprzętowe oraz bezpieczne zarządzanie hasłami.
5. Bezpieczeństwo systemów i urządzeń, w tym zasady bezpiecznego korzystania z urządzeń służbowych i systemów informatycznych, zakaz instalacji nieautoryzowanego oprogramowania oraz regularna aktualizacja systemów operacyjnych i aplikacji.
6. Reagowanie na incydenty bezpieczeństwa, w tym procedury zgłaszania incydentów bezpieczeństwa oraz sposoby ich dokumentowania, identyfikowanie potencjalnych incydentów i podejmowanie właściwych działań, współpraca z zespołem IT w celu rozwiązania problemów związanych z bezpieczeństwem.
7. Sposoby budowania kultury bezpieczeństwa, w tym metody ciągłego doskonalenia umiejętności, dzielenie się wiedzą, audyty wewnętrzne, promocja bezpieczeństwa informacji w codziennej pracy i zachęcanie innych pracowników do przestrzegania najlepszych praktyk, współtworzenie środowiska pracy, w którym bezpieczeństwo jest traktowane jako priorytet.
8. Testy socjotechniczne weryfikujące świadomość zagrożeń i reakcji specjalistów posiadających wyznaczone obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami.

Testy muszą obejmować co najmniej:

- umiejętność wykorzystania wiedzy zdobytej podczas kursu w praktyce,
- zdolność do identyfikacji prób ataków socjotechnicznych i podejmowania odpowiednich kroków w celu ich zneutralizowania,
- postępowanie zgodnie z procedurami i rolami w SZBI,
- analizę wyników testów i wyciąganie wniosków z popełnionych błędów w celu poprawy przyszłych reakcji.

Zamawiający oczekuje przeprowadzenia **jednej rundy testów socjotechnicznych**. Wykonawca przedstawi Zamawiającemu pisemne podsumowanie wyników testów.

Organizacja szkolenia:

1. Szkolenie zostanie przeprowadzone w trybie **stacjonarnym, w siedzibie Zamawiającego**.
2. Szkoleniem zostaną objęci **wszyscy pracownicy Zamawiającego – około 44 osoby**.
3. W celu zapewnienia **ciągłości funkcjonowania Zamawiającego oraz możliwości wykonywania bieżących obowiązków służbowych**, szkolenie zostanie przeprowadzone w ramach **4 odrębnych edycji**, dla grup liczących około **11 osób każda**.
4. Każda z grup zostanie objęta **pełnym i jednakowym zakresem tematycznym szkolenia**.
5. Czas trwania jednej edycji szkolenia wynosi **minimum 3 godziny zegarowe**, łącznie z przerwami. Łączny minimalny wymiar realizacji szkoleń wynosi **12 godzin zegarowych** (4 edycje × minimum 3 godziny).
6. Podział pracowników na poszczególne grupy zostanie dokonany przez Zamawiającego z uwzględnieniem struktury organizacyjnej, zakresu obowiązków pracowników oraz konieczności zapewnienia ciągłości działania poszczególnych komórek organizacyjnych i procesów realizowanych przez Zamawiającego.
7. Terminy poszczególnych edycji zostaną uzgodnione z Zamawiającym. Zamawiający dopuszcza przeprowadzenie poszczególnych edycji w różnych dniach.
8. Szkolenie musi być prowadzone **w języku polskim**.
9. W przypadku nieobecności pracownika podczas wyznaczonej edycji Zamawiający dopuszcza możliwość przeprowadzenia dla niego szkolenia uzupełniającego **w formie zdalnej (online)**, obejmującego pełny wymagany zakres tematyczny.

Oświadczenie Wykonawcy.

Oświadczam, że składając ofertę świadom jestem jej złożenia i zapewniam, że wykonam zamówienie zgodnie z oczekiwaniami Zamawiającego.

Składając ofertę oświadczam, że spełniam warunki udziału w postępowaniu.

Oświadczam, że wykonam zamówienie zgodnie z wymaganiami zawartymi w niniejszym Opisie Przedmiotu Zamówienia.

....., dnia