Cyberbezpieczne Wodociągi

Załącznik nr 1 do SWZ

Szczegółowy Opis Przedmiotu Zamówienia
Zarządzanie cyberbezpieczeństwem i rozwój kompetencji – zakres odpowiadający Części II pierwotnego postępowania"

Część II obejmuje działania z zakresu zarządzania cyberbezpieczeństwem i rozwoju kompetencji, mające na celu wdrożenie oraz utrzymanie skutecznego systemu zarządzania bezpieczeństwem informacji, zapewnienie ciągłości działania, wsparcie procesów zarządzania ryzykiem i zgodnością oraz podniesienie poziomu świadomości i kompetencji pracowników Zamawiającego. Realizacja zadań powinna zapewniać zgodność z wymaganiami przepisów z zakresu krajowego systemu cyberbezpieczeństwa obowiązującymi na dzień realizacji zamówienia, z uwzględnieniem wymagań wynikających z dyrektywy NIS2 oraz norm ISO/IEC 27001 i ISO 22301

Wszystkie Zadania od 1 do 10 objęte przedmiotem zamówienia to:

Zadanie 1: System Zarządzania Bezpieczeństwem Informacji (SZBI)

1. Przedmiot zamówienia
   Przedmiotem zamówienia jest opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z wymaganiami normy ISO/IEC 27001 oraz ustawy o KSC.
2. W ramach przedmiotu zamówienia Wykonawca opracuje, dostarczy i wdroży Zamawiającemu dokumentację SZBI.
   1) Dokumentacja SZBI obejmuje co najmniej:
      a) Politykę Bezpieczeństwa Informacji,
      b) dokumentację dotyczącą ochrony danych osobowych w zakresie powiązanym z SZBI,
      c) zasady i procedury zarządzania bezpieczeństwem systemów teleinformatycznych,
      d) analizę ryzyka i plan postępowania z ryzykiem,
      e) polityki, procedury, rejestry i pozostałą dokumentację niezbędną do funkcjonowania SZBI zgodnie z wymaganiami określonymi w SOPZ."
   2) Dokumentacja musi być zgodna z:
      a) ISO/IEC 27001,
      b) ISO 22301,
      c) ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity: Dz. U. z 2026 r. poz. 20 ze zm.), zwaną dalej ustawą o KSC,
      d) rozporządzeniem 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 (Dz. U. UE. L. z 2016 r. Nr 119, s. 1 ze zm.), zwanym dalej RODO,
      e) rozporządzeniem 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. z 2024 r. poz. 773), zwanym dalej KRI.
3. Analiza ryzyka
   Przeprowadzenie analizy ryzyka bezpieczeństwa informacji powinno obejmować identyfikację, ocenę i postępowanie z ryzykiem dla systemów IT/OT/ICS Zamawiającego.
4. Wdrożenie SZBI powinno obejmować:
   1) wdrożenie polityk, procedur i środków bezpieczeństwa wynikających z analizy ryzyka;

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

2) szkolenie personelu z zakresu opracowanej dokumentacji SZBI.

Zadanie 2: Plany ciągłości działania i odtwarzania po awarii – BCP/DRP

1. Przedmiot zamówienia
   Przedmiotem zamówienia jest opracowanie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP) dla systemów teleinformatycznych (STI) Zamawiającego.
2. Zakres BCP obejmujący w szczególności:
   1) opracowanie planu ciągłości działania obejmującego krytyczne procesy biznesowe i usługi (dostawy wody, zarządzanie infrastrukturą),
   2) identyfikację zasobów krytycznych,
   3) określenie RTO i RPO.
3. Zakres DRP obejmujący w szczególności:
   1) opracowanie planu odtwarzania po awarii dla infrastruktury IT/OT,
   2) procedury przywracania usług,
   3) kolejność odtwarzania systemów,
   4) listę kontaktów awaryjnych.
4. Testy procedur obejmujące w szczególności:
   1) przeprowadzenie testów opracowanych planów (ćwiczenia, testy tabletop lub symulacje),
   2) dokumentację wyników testów.
5. Regularna aktualizacja obejmująca w szczególności:
   1) procedurę regularnej aktualizacji BCP/DRP,
   2) zdefiniowanie harmonogramu przeglądów (min. raz w roku lub po istotnych zmianach infrastruktury).
6. Integracja z SZBI
   Plany BCP/DRP powinny być zintegrowane z Systemem Zarządzania Bezpieczeństwem Informacji (SZBI) i Systemem Zarządzania Ciągłością Działania (SZCD).
7. Zgodność z regulacjami:
   1) normą ISO 22301 (SZCD),
   2) normą ISO/IEC 27001,
   3) ustawą o KSC,
   4) wymaganiami wynikającymi z ustawy o KSC oraz innych przepisów z zakresu cyberbezpieczeństwa mających zastosowanie do Zamawiającego, stosownie do jego statusu prawnego .

Zadanie 3: System Zarządzania Ciągłością Działania (SZCD)

1. Przedmiot zamówienia
   Przedmiotem zamówienia jest opracowanie i wdrożenie Systemu Zarządzania Ciągłością Działania (SZCD) zgodnego z normą ISO 22301.
2. Polityka ciągłości działania obejmująca w szczególności:
   1) opracowanie i wdrożenie Polityki zarządzania ciągłością działania Zamawiającego,
   2) określenie celów, zakresu i odpowiedzialności w obszarze ciągłości działania.
3. Procedury zarządzania incydentami obejmujące w szczególności:

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

opracowanie i wdrożenie procedur zarządzania incydentami cyberbezpieczeństwa: identyfikacja, klasyfikacja, reakcja, eskalacja, raportowanie.

4. Integracja z BCP/DRP
   Należy dokonać integracji SZCD z planami BCP i DRP oraz z Systemem Zarządzania Bezpieczeństwem Informacji (SZBI).
5. Szkolenie personelu
   Szkolenie personelu kluczowego z zakresu procedur SZCD i reagowania na incydenty.
6. Zgodność z regulacjami:
   1) normą ISO 22301,
   2) normą ISO/IEC 27001,
   3) ustawa o KSC,
   4) KRI,
   5) wymagania Operatora Usługi Kluczowej.

Zadanie 4: System klasy GRC (GOVERNANCE, RISK AND COMPLIANCE)

1. Przedmiot zamówienia
   Przedmiotem zamówienia jest dostawa systemu klasy GRC (Governance, Risk and Compliance), który stanowić będzie centralną platformę do zarządzania ładem organizacyjnym, ryzykiem, zgodnością regulacyjną oraz procesami bezpieczeństwa informacji i cyberbezpieczeństwa w środowisku IT/OT Zamawiającego. Dostarczone rozwiązanie ma wspierać realizację obowiązków wynikających z wymagań KSC, NIS2, RODO, ISO/IEC 27001, ISO 22301 oraz KRI, zapewniając jednolite środowisko do ewidencji, nadzoru, raportowania, obsługi incydentów, zarządzania dokumentacją, audytami, działaniami korygującymi oraz planami ciągłości działania i odtwarzania po awarii.
2. Wymagania minimalne dostarczonego rozwiązania
   1) Rozwiązanie musi umożliwiać centralne zarządzanie procesami związanymi z:
      a) bezpieczeństwem informacji,
      b) cyberbezpieczeństwem,
      c) zgodnością regulacyjną,
      d) zarządzaniem ryzykiem,
      e) incydentami, podatnościami,
      f) audytami,
      g) działaniami korygującymi,
      h) dokumentacją organizacyjną i techniczną,
      i) procesami SZBI i SZCD oraz planami BCP i DRP.
   2) System musi zapewniać:
      a) centralną konsolę administracyjną,
      b) dostęp przez przeglądarkę internetową,
      c) wielopoziomowe zarządzanie uprawnieniami,
      d) obsługę wielu ról administracyjnych i użytkowników
      e) możliwość pracy w modelu on-premise lub chmurowym,
      f) centralne zarządzanie dokumentacją bezpieczeństwa, w tym repozytorium dokumentów, wersjonowanie, historię zmian, workflow akceptacji, publikację dokumentów,
      g) nadawanie uprawnień dostępu,
      h) harmonogramy przeglądów,
      i) możliwość potwierdzania zapoznania się z dokumentacją przez użytkowników,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

j) dashboardy bezpieczeństwa i zgodności,
k) graficzną prezentację poziomu ryzyka,
l) raporty bezpieczeństwa i zgodności,
m) raporty dla kierownictwa i audytorów,
n) definiowanie i monitorowanie wskaźników KPI/KRI.

3) Rozwiązanie musi umożliwiać prowadzenie centralnych rejestrów obejmujących co najmniej:
   a) rejestr ryzyka,
   b) rejestr incydentów,
   c) rejestr podatności,
   d) rejestr aktywów,
   e) rejestr audytów,
   f) rejestr działań korygujących,
   g) rejestr polityk i procedur,
   h) rejestr zgodności regulacyjnej,
   i) rejestr wyjątków bezpieczeństwa.
4) W obszarze zarządzania ryzykiem system musi wspierać:
   a) identyfikację, analizę i ocenę ryzyka,
   b) definiowanie właścicieli ryzyka,
   c) prowadzenie macierzy ryzyka,
   d) ocenę wpływu i prawdopodobieństwa,
   e) definiowanie planów postępowania z ryzykiem,
   f) monitorowanie poziomu ryzyka i terminów przeglądów,
   g) obsługę procesów akceptacji ryzyka.
5) W obszarze zarządzania zgodnością system musi wspierać:
   a) monitorowanie realizacji wymagań regulacyjnych,
   b) przypisywanie wymagań do procesów, aktywów i dokumentacji,
   c) prowadzenie ewidencji zgodności,
   d) monitorowanie terminów przeglądów i aktualizacji,
   e) generowanie raportów zgodności,
   f) nadzór nad działaniami naprawczymi.
6) Rozwiązanie musi wspierać:
   a) realizację audytów bezpieczeństwa poprzez planowanie audytów,
   b) definiowanie zakresów,
   c) rejestrowanie ustaleń i niezgodności,
   d) przypisywanie działań naprawczych,
   e) monitorowanie statusu zaleceń,
   f) generowanie raportów audytowych,
   g) procesy SZBI i SZCD, w tym obsługę analiz BIA,
   h) zarządzanie planami BCP/DRP,
   i) harmonogramowanie testów i przeglądów,
   j) monitorowanie skuteczności procesów,
   k) prowadzenie kompletnej dokumentacji systemowej związanej z utrzymaniem bezpieczeństwa i ciągłości działania.
7) System musi umożliwiać:
   a) obsługę incydentów bezpieczeństwa obejmującą rejestrowanie incydentów, klasyfikację, nadawanie priorytetów,
   b) przypisywanie właścicieli,
   c) prowadzenie działań obsługowych i naprawczych,
   d) monitorowanie statusu,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

e) raportowanie incydentów bezpieczeństwa, z uwzględnieniem obowiązków raportowych wynikających z KSC i NIS2.

8) W zakresie bezpieczeństwa rozwiązanie musi wspierać:
   a) mechanizmy RBAC, MFA, szyfrowanie komunikacji,
   b) rejestrowanie działań użytkowników i zdarzeń administracyjnych,
   c) backup konfiguracji i danych,
   d) pracę w środowisku wysokiej dostępności (HA),
   e) dostarczanie aktualizacji bezpieczeństwa systemu.
9) Rozwiązanie musi wspierać:
   realizację wymagań związanych z NIS2, KSC, ISO/IEC 27001, ISO 22301, RODO, KRI- w zakresie mającym zastosowanie do Zamawiającego lub przyjętym przez Zamawiającego jako wymagania referencyjne oraz wymaganiami cyberbezpieczeństwa infrastruktury krytycznej.
10) W ramach wdrożenia Wykonawca zobowiązany jest do zapewnienia minimum 24 miesięcy wsparcia technicznego i dostępu do aktualizacji oraz poprawek bezpieczeństwa.

Zadanie 5: Wdrożenie Systemu klasy GRC

1. Przedmiot zamówienia
   Przedmiotem zamówienia jest instalacja, konfiguracja, uruchomienie i dostosowanie rozwiązania do środowiska organizacyjnego i technicznego Zamawiającego oraz dostarczenie Zamawiającemu dokumentacji powdrożeniowej.
2. Zakres wdrożenia
   Wdrożenie obejmuje co najmniej:
   1) przygotowanie środowiska docelowego (produkcyjnego) oraz testowego (jeśli wymagane) zgodnie z wymaganiami technicznym systemu,
   2) instalację komponentów systemu GRC na wskazanej infrastrukturze (sprzętowej lub wirtualnej),
   3) konfigurację modułów: zarządzania ryzykiem, zgodności, kontroli, incydentów, polityk, audytu, ciągłości działania,
   4) odwzorowanie struktury organizacyjnej Zamawiającego w systemie (komórki, stanowiska, relacje),
   5) definicję i konfigurację ról systemowych oraz przypisanie uprawnień zgodnie z wymaganiami Zamawiającego,
   6) utworzenie wymaganych rejestrów: ryzyk, kontroli, incydentów, podatności, aktywów, BCP/DRP, niezgodności, działań naprawczych,
   7) skonfigurowanie workflow procesowych (przepływów procesowych) np. akceptacja ryzyka, zgłaszanie incydentów, obieg zadań naprawczych,
   8) przygotowanie raportów i widoków dashboardów zgodnie z potrzebami Zamawiającego (co najmniej raporty dla kierownictwa, zespołu bezpieczeństwa, audytorów).
3. Dokumentacja powdrożeniowa
   1) Wykonawca zobowiązany jest dostarczyć:
      a) dokumentację administracyjną – opis czynności administracyjnych, procedury backupu, odtwarzania, monitorowania systemu,
      b) dokumentację użytkową – instrukcję obsługi dla użytkowników końcowych (wg ról: zarządzający ryzykiem, audytor, właściciel kontroli, użytkownik zgłaszający incydent),
      c) dokumentację konfiguracyjną – parametry konfiguracji systemu (role, workflow, słowniki, integracje).

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

2) Wykonawca zobowiązany jest dostarczyć Zamawiającemu dokumentację w formie elektronicznej (PDF, edytowalna) oraz w wersji drukowanej (co najmniej 1 egzemplarz).

Zadanie 6: Szkolenia dla administratorów Systemu klasy GRC

1. Przedmiot zamówienia
   Przedmiotem zamówienia jest przeprowadzenie szkolenia dla administratorów systemu klasy GRC, które będzie miało charakter praktyczny i przygotuje wskazanych przez Zamawiającego pracowników do samodzielnego utrzymania, nadzoru i bieżącej obsługi rozwiązania.
2. Minimalny zakres szkolenia obejmuje w szczególności:
   1) konfigurację parametrów administracyjnych, w tym:
      a) ustawienia systemowe,
      b) konfiguracja słowników,
      c) definiowanie typów ryzyk, kategorii incydentów, matryc ryzyka;
   2) zarządzanie użytkownikami, rolami i uprawnieniami, w tym:
      a) tworzenie i blokowanie kont,
      b) przypisywanie i modyfikacja ról,
      c) definiowanie uprawnień szczegółowych;
   3) administrowanie rejestrami i słownikami systemowymi, w tym:
      a) zarządzanie rejestrami (ryzyka, kontrole, incydenty),
      b) dodawanie nowych pól,
      c) modyfikacja słowników;
   4) obsługę workflow, w tym:
      a) konfiguracja przepływów,
      b) definiowanie ścieżek akceptacji,
      c) zarządzanie zadaniami i powiadomieniami;
   5) generowanie raportów i dashboardów, w tym:
      a) tworzenie własnych raportów,
      b) modyfikacja istniejących dashboardów,
      c) eksport danych;
   6) monitorowanie działania systemu, w tym:
      a) sprawdzanie logów, wydajności, stanu usług,
      b) identyfikacja problemów;
   7) podstawowe czynności utrzymaniowe, w tym:
      a) backup i odtwarzanie konfiguracji,
      b) aktualizacje systemu;
   8) dobre praktyki eksploatacyjne, w tym zalecenia dotyczące:
      a) cyklu życia konfiguracji,
      b) zarządzania zmianami w systemie,
      c) bezpieczeństwa administracji.
3. Realizacja szkolenia
   1) Szkolenie powinno być realizowane z wykorzystaniem skonfigurowanego środowiska Zamawiającego (środowisko testowe lub produkcyjne).
   2) Czas trwania: minimum 2 dni szkoleniowe, w tym co najmniej 70% czasu na ćwiczenia praktyczne.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

3) Liczba uczestników: do 4 osób wskazanych przez Zamawiającego (w tym przyszli administratorzy).
4) Miejsce szkolenia: siedziba Zamawiającego lub zdalnie – do uzgodnienia.
5) Język szkolenia: polski.

4. Materiały szkoleniowe i zakończenie
   1) Po zakończeniu szkolenia Wykonawca przekazuje:
      a) materiały szkoleniowe w formie elektronicznej (prezentacje, instrukcje do ćwiczeń, zestawienia komend / czynności administracyjnych),
      b) instrukcję administracyjną – uszczegółowioną wersję dokumentacji administracyjnej, dostosowaną do zrealizowanego zakresu konfiguracji.
   2) Szkolenie kończy się wydaniem imiennych zaświadczeń / certyfikatów ukończenia szkolenia dla uczestników, zawierających zakres tematyczny i wymiar godzin.

Zadanie 7: Dostarczenie platformy szkoleniowej do realizacji podstawowych szkoleń z zakresu cyberbezpieczeństwa dla pracowników

1. Przedmiot zamówienia
   Przedmiotem zamówienia jest dostawa, konfiguracja oraz uruchomienie platformy szkoleniowej przeznaczonej do realizacji szkoleń e-learningowych z zakresu cyberbezpieczeństwa dla pracowników Zamawiającego.
2. Wymagane funkcjonalności platformy
   1) Platforma musi umożliwiać prowadzenie szkoleń w formie elektronicznej z wykorzystaniem:
      a) materiałów multimedialnych,
      b) prezentacji,
      c) materiałów interaktywnych,
      d) filmów szkoleniowych,
      e) testów wiedzy,
      f) mechanizmów raportowania i monitorowania postępów uczestników.
   2) Rozwiązanie musi zapewniać co najmniej następujące funkcjonalności:
      a) centralne Zarządzanie procesem szkoleniowym,
      b) zarządzanie użytkownikami i grupami szkoleniowymi,
      c) możliwość przypisywania szkoleń do użytkowników / grup,
      d) monitorowanie realizacji szkoleń przez uczestników,
      e) monitorowanie wyników, tj. śledzenie wyników testów i aktywności,
      f) raportowanie, tj. generowanie raportów i zestawień (w tym eksport),
      g) certyfikacja, tj. generowanie certyfikatów lub potwierdzeń ukończenia szkolenia,
      h) dostępność, tj. dostęp z poziomu przeglądarki internetowej, bez instalacji dodatkowego oprogramowania u użytkownika końcowego,
      i) praca zdalna, tj. możliwość korzystania z platformy zdalnie (Internet),
      j) harmonogramowanie, tj. planowanie terminów i przypomnień o szkoleniach,
      k) testy wiedzy, tj. prowadzenie testów (wielokrotnego wyboru, prawda/fałsz, otwarte),
      l) śledzenie aktywności, tj. logowanie aktywności użytkowników (czas, postępy, wyniki),
      m) raportowanie wyników testów, tj. tworzenie szczegółowych raportów z wyników testów na poziomie użytkownika i grupy,
      n) archiwizacja wyników szkoleniowych (co najmniej 5 lat wstecz),
      o) uprawnienia administracyjne, tj. obsługa wielu poziomów uprawnień (administrator główny, kierownik szkoleń, trener, użytkownik).
3. Zakres merytoryczny szkoleń (treści podstawowe)

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

1) Platforma musi umożliwiać prowadzenie szkoleń obejmujących co najmniej następujące tematy:
   a) bezpieczeństwo haseł,
   b) phishing i socjotechnika,
   c) bezpieczne korzystanie z poczty elektronicznej,
   d) ochrona danych osobowych (RODO),
   e) bezpieczna praca zdalna,
   f) bezpieczne korzystanie z urządzeń mobilnych,
   g) zgłaszanie incydentów bezpieczeństwa,
   h) podstawowe zasady ochrony informacji.
2) Obowiązki Wykonawcy
   W ramach realizacji zamówienia Wykonawca zobowiązany jest do:
   a) dostarczenia gotowej do pracy platformy szkoleniowej (model SaaS lub on-premise),
   b) przygotowania i udostępnienia materiałów szkoleniowych,
   c) konfiguracji użytkowników oraz uprawnień (co najmniej dla wydziałów / stanowisk wskazanych przez Zamawiającego),
   d) przeprowadzenia konfiguracji raportowania (przygotowanie szablonów raportów według wzorów Zamawiającego),
   e) przygotowania instrukcji użytkowania platformy (dla uczestników i administratorów szkoleń),
   f) przekazania dokumentacji administracyjnej i użytkowej,
   g) przeprowadzenia konsultacji dla przedstawicieli Zamawiającego (online lub stacjonarnie, min. 2 godziny),
   h) zapewnienia wsparcia technicznego w okresie wdrożenia (co najmniej w godzinach pracy Zamawiającego).

Zadanie 8: Realizacja stacjonarnych szkoleń podstawowych z zakresu cyberbezpieczeństwa dla pracowników

1. Przedmiot zamówienia
   Przedmiotem zamówienia jest organizacja oraz przeprowadzenie stacjonarnych szkoleń z zakresu cyberbezpieczeństwa dla pracowników Zamawiającego. Szkolenia muszą obejmować zarówno część teoretyczną, jak i praktyczne przykłady zagrożeń oraz incydentów bezpieczeństwa związanych z codzienną pracą użytkowników.
2. Minimalny zakres merytoryczny
   Szkolenie musi obejmować co najmniej następujące zagadnienia:

Lp.	Temat	Minimalny zakres
1	Podstawowe zagadnienia cyberbezpieczeństwa	Kluczowe pojęcia, aktualne zagrożenia
2	Bezpieczeństwo haseł	Zasady tworzenia i przechowywania haseł, uwierzytelnianie wieloskładnikowe
3	Phishing	Rozpoznawanie wiadomości phishingowych, przykłady ataków
4	Socjotechnika	Metody manipulacji, preteksty, wyłudzanie informacji
5	Bezpieczne korzystanie z poczty elektronicznej	Szyfrowanie, załączniki, linki, certyfikaty
6	Ochrona danych osobowych	RODO, obowiązki pracownika, zgłaszanie naruszeń

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

7	Bezpieczna organizacja pracy zdalnej	VPN, szyfrowanie, czyste biurko, zasady BYOD
8	Bezpieczne korzystanie z urządzeń mobilnych	Aktualizacje, aplikacje, blokady ekranu, zgubienie urządzenia
9	Rozpoznawanie zagrożeń bezpieczeństwa	Typowe ataki, symptomy włamania, alerty
10	Zasady zgłaszania incydentów bezpieczeństwa	Procedury, kontakt do CSIRT, zasady eskalacji
11	Podstawowe zasady ochrony informacji	Klasyfikacja, udostępnianie, niszczenie dokumentów

3. Wymagania dotyczące kadry i materiałów
   1) Szkolenia muszą być prowadzone przez specjalistów posiadających wiedzę merytoryczną oraz doświadczenie praktyczne w zakresie cyberbezpieczeństwa (min. 2 lata praktyki w obszarze bezpieczeństwa IT lub audytu).
   2) Każdy trener powinien przedstawić CV / referencje na żądanie Zamawiającego.
   3) Szkolenia powinny być dostosowane do specyfiki organizacji Zamawiającego oraz zagrożeń związanych z wykonywaniem obowiązków służbowych przez pracowników (na podstawie wstępnej ankiety lub rozmowy z Zamawiającym).
   4) Materiały dydaktyczne (prezentacje, ćwiczenia, case study) należy przedstawić Zamawiającemu w formie elektronicznej.
4. Obowiązki Wykonawcy

   W ramach realizacji usługi Wykonawca zobowiązany jest do:
   1) przygotowania programu szkolenia (scenariusz, harmonogram),
   2) zapewnienia kadry szkoleniowej,
   3) przygotowania materiałów dydaktycznych (dla każdego uczestnika),
   4) przeprowadzenia szkolenia (zgodnie z ustalonym terminem i lokalizacją),
   5) przeprowadzenia testów wiedzy – test końcowy powinien zawierać min. 10 pytań,
   6) przygotowania dokumentacji obecności (listy obecności podpisane przez uczestników),
   7) wydania certyfikatów lub potwierdzeń ukończenia szkolenia (imienne, z podaniem zakresu i liczby godzin).
5. Dokumentowanie szkolenia

   Wykonawca zobowiązany jest do zapewnienia dokumentowania realizacji szkolenia, w szczególności:
   1) list obecności (dla każdej grupy szkoleniowej),
   2) materiałów szkoleniowych (przekazanych Zamawiającemu),
   3) wyników testów wiedzy – (anonimowo lub imiennie wg potrzeb),
   4) raportów z przeprowadzonych szkoleń – zawierających co najmniej:
      a) datę i miejsce szkolenia,
      b) liczbę uczestników,
      c) program i realizację tematów,
      d) ocenę poziomu wiedzy,
      e) wnioski i rekomendacje dla Zamawiającego.

Zadanie 9: Szkolenie z zakresu cyberbezpieczeństwa dla kadry zarządzającej – platforma szkoleniowa

1. Przedmiot zamówienia

   Przedmiotem zamówienia jest dostawa, konfiguracja oraz uruchomienie platformy szkoleniowej przeznaczonej do realizacji szkoleń e-learningowych z zakresu cyberbezpieczeństwa dla kadry zarządzającej Zamawiającego (kierownicy, dyrektorzy, członkowie kierownictwa wyższego

szczebla, osoby odpowiedzialne za nadzór nad bezpieczeństwem informacji). Platforma musi uwzględniać specyficzne potrzeby kadry zarządzającej – w szczególności ukierunkowanie na aspekty strategiczne, decyzyjne, zarządcze i nadzorcze.

2. Wymagania funkcjonalności platformy (dla kadry zarządzającej)

Platforma (lub jej dedykowany moduł) musi zapewniać co najmniej takie same funkcjonalności jak w Zadaniu 7, a dodatkowo:

1) raportowanie zbiorcze, tj. możliwość generowania skonsolidowanych raportów z poziomu realizacji szkoleń przez podległe zespoły (dla menedżerów),
2) dashboard zarządczy, tj. widok kluczowych wskaźników (KPI) dotyczących kultury bezpieczeństwa w organizacji,
3) poziomy uprawnień, tj. rozróżnienie roli „menedżer szkoleń" (może przypisywać szkolenia, przeglądać wyniki swojego działu),

3. Zakres merytoryczny szkoleń dla kadry zarządzającej

Szkolenia muszą obejmować co najmniej następujące zagadnienia (z naciskiem na perspektywę zarządczą):

Lp.	Temat	Minimalny zakres
1	Rola kierownictwa w systemie zarządzania bezpieczeństwem informacji (SZBI)	Obowiązki lidera, nadzór, alokacja zasobów, polityki bezpieczeństwa
2	Zarządzanie ryzykiem cyberbezpieczeństwa na poziomie strategicznym	Identyfikacja ryzyk strategicznych, akceptacja ryzyka, apetyt na ryzyko, raportowanie do zarządu
3	Zgodność i wymagania regulacyjne (KSC, RODO, NIS2, ISO 27001)	Obowiązki podmiotu kluczowego / usługodawcy, odpowiedzialność kierownictwa, kary i sankcje
4	Zarządzanie incydentami – perspektywa zarządcza	Procedury eskalacji, zarządzanie kryzysowe, komunikacja z interesariuszami, powiadamianie regulatorów
5	Ciągłość działania (BCP / DRP) – aspekty zarządcze	Plany ciągłości, testowanie, decyzje o uruchomieniu procedur, budżet na odtwarzanie
6	Nadzór nad bezpieczeństwem dostawców i stron trzecich	Ocena dostawców, klauzule umowne, audyty, monitoring
7	Kultura bezpieczeństwa i świadomość w organizacji	Budowanie programu świadomości, szkolenia pracowników, mierzenie kultury
8	Budżetowanie i inwestycje w cyberbezpieczeństwo	ROI, analiza kosztów i korzyści, priorytetyzacja wydatków
9	Aspekty prawne i odpowiedzialność kierownictwa	Ustawa o KSC, kodeks spółek handlowych, odpowiedzialność za naruszenia
10	Komunikacja kryzysowa i zarządzanie reputacją	Wzorce postępowania, komunikaty wewnętrzne i zewnętrzne, PR w kryzysie

4. Obowiązki Wykonawcy

W ramach realizacji zamówienia dla kadry zarządzającej Wykonawca zobowiązany jest do:

1) dostarczenia platformy / udostępnienia dedykowanego modułu (może być to samo rozwiązanie co w Zadaniu 7, ale z osobnym katalogiem szkoleń i dostępami),
2) przygotowania materiałów szkoleniowych dostosowanych do poziomu kadry zarządzającej (studia przypadków, analiza decyzyjna, symulacje),
3) konfiguracji ról i uprawnień dla kierownictwa (np. możliwość wglądu w wyniki podległych działów),
4) przeprowadzenia konsultacji dla przedstawicieli kadry zarządzającej (online lub stacjonarnie, min. 2 godziny),

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

5) przygotowania instrukcji użytkowania w wersji „dla menedżera”,
6) zapewnienia wsparcia technicznego,

Zadanie 10: Szkolenie z zakresu cyberbezpieczeństwa dla kadry zarządzającej – szkolenie stacjonarne

1. Przedmiot zamówienia
   Przedmiotem zamówienia jest organizacja oraz przeprowadzenie stacjonarnych szkoleń z zakresu cyberbezpieczeństwa dedykowanych kadrze zarządzającej Zamawiającego (osoby kierownicze, dyrektorzy, członkowie zarządu, pełnomocnicy ds. bezpieczeństwa). Szkolenie musi łączyć część teoretyczną z warsztatami praktycznymi, case study oraz symulacjami podejmowania decyzji w sytuacjach kryzysowych.
2. Minimalny zakres merytoryczny
   Szkolenie stacjonarne dla kadry zarządzającej musi obejmować co najmniej:

Lp.	Temat	Forma realizacji
1	Strategiczne zarządzanie cyberbezpieczeństwem	Wykład + dyskusja
2	Identyfikacja i ocena ryzyka cyberbezpieczeństwa	Warsztat analizy ryzyka na przykładzie organizacji
3	Obowiązki prawne kierownictwa (KSC, NIS2, RODO)	Case study – odpowiedzialność
4	Zarządzanie incydentem – symulacja kryzysowa	Gra decyzyjna / symulacja
5	Zarządzanie ciągłością działania (BCP) dla kadry	Ćwiczenie tablicowe – uruchomienie planu
6	Nadzór nad bezpieczeństwem łańcucha dostaw	Analiza umów, ocena dostawców
7	Budżetowanie i raportowanie cyberbezpieczeństwa	Praktyczne szablony KPI i KRI
8	Komunikacja kryzysowa i zarządzanie reputacją	Symulacja odpowiedzi na incydent medialny

   Dodatkowo szkolenie powinno zawierać praktyczne przykłady zagrożeń oraz incydentów bezpieczeństwa z perspektywy decyzyjnej (np. atak ransomware – podjąć okup czy nie, powiadomić regulatora czy nie).
3. Wymagania dotyczące kadry i materiałów
   1) Trenerzy prowadzący szkolenie dla kadry zarządzającej muszą posiadać udokumentowane doświadczenie w prowadzeniu szkoleń dla kierownictwa wyższego szczebla oraz wiedzę z zakresu zarządzania ryzykiem, compliance i strategii cyberbezpieczeństwa.
   2) Materiały dydaktyczne muszą być dostosowane do poziomu kadry zarządzającej: skrócone, syntetyczne, z naciskiem na wnioski i rekomendacje (tzw. briefing executives).
4. Obowiązki Wykonawcy
   Wykonawca zobowiązany jest do:
   1) przygotowania programu szkolenia (uwzględniającego specyfikę Zamawiającego – na podstawie wywiadu),
   2) zapewnienia kadry szkoleniowej,
   3) przygotowania materiałów dydaktycznych (w formie elektronicznej oraz papierowe skrypty),

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

4) przeprowadzenia szkolenia (stacjonarnie, w lokalizacji wskazanej przez Zamawiającego),
5) przeprowadzenia testów wiedzy / oceny przed i po (krótki quiz, ocena efektywności),
6) przygotowania dokumentacji obecności (listy obecności),
7) przekazania materiałów szkoleniowych każdemu uczestnikowi,
8) przygotowania raportu z realizacji szkolenia,
9) wydania imiennych certyfikatów ukończenia szkolenia (z określeniem liczby godzin i zakresu).

5. Dokumentowanie szkolenia
Dokumentacja powinna zawierać:
1) listy obecności (podpisane przez uczestników),
2) materiały szkoleniowe (przekazane Zamawiającemu),
3) wyniki testów wiedzy,
4) raport końcowy – obejmujący co najmniej:
a) program i harmonogram,
b) liczbę uczestników (z podziałem na stanowiska),
c) wyniki oceny szkolenia (ankiety satysfakcji, jeśli zamawiający określi taką potrzebę),
d) wnioski i rekomendacje dla kierownictwa Zamawiającego.
6. Szkolenia prowadzą osoby spełniające wymagania dotyczące personelu określone dla Części II w SWZ
7. Wszystkie Zadania od 1 do 10 objęte Częścią II należy zrealizować w terminie określonym w SWZ oraz umowie.”

WYMAGANIA WSPÓLNE DOTYCZĄCE ETAPOWEGO PRZEKAZYWANIA REZULTATÓW I WSPÓŁPRACY Z WYKONAWCĄ AUDYTU

1. Realizacja przedmiotu zamówienia odbywa się etapowo, zgodnie z harmonogramem rzeczowo-finansowym uzgodnionym z Zamawiającym. Wykonawca zobowiązany jest do sukcesywnego przekazywania Zamawiającemu produktów i rezultatów poszczególnych Zadań niezwłocznie po ich wykonaniu, bez oczekiwania na zakończenie realizacji całości przedmiotu zamówienia.

2. Każdy rezultat danego Zadania powinien zostać przekazany wraz z dokumentacją i dowodami jego wykonania w zakresie umożliwiającym Zamawiającemu bieżącą weryfikację oraz późniejszą ocenę w ramach audytu cyberbezpieczeństwa.

3. Wykonawca zobowiązany jest do współpracy z Zamawiającym oraz wykonawcą audytu cyberbezpieczeństwa realizowanego w ramach Projektu, w zakresie dotyczącym produktów i rezultatów objętych niniejszym zamówieniem.

4. Współpraca obejmuje w szczególności: sukcesywne udostępnianie dokumentacji, polityk, procedur, rejestrów i innych rezultatów prac; przekazywanie informacji o zakończeniu poszczególnych Zadań lub etapów; udzielanie wyjaśnień dotyczących wykonanych prac i wdrożonych rozwiązań; przekazywanie informacji i dowodów niezbędnych do oceny rezultatów; współpracę przy wyjaśnianiu uwag lub niezgodności stwierdzonych w toku audytu w zakresie odnoszącym się do prac wykonanych przez Wykonawcę.

5. Obowiązek współpracy z wykonawcą audytu nie powoduje rozszerzenia zakresu rzeczowego zamówienia ani obowiązku wykonania świadczeń niewchodzących w zakres SOPZ i Umowy.