

Załącznik nr 2 do Zapytania Ofertowego

Szczegółowy Opis Przedmiotu zamówienia

**Zakup szkoleń dla kadry kierowniczej oraz personelu medycznego i administracyjnego - dostęp do platformy dla 1000 użytkowników w Wojewódzkim Szpitalu Specjalistycznym nr 2 w Jastrzębiu-Zdroju - powtórzenie
BZP.38.383-12.26**

Zakupy realizowany w ramach projektu „Przyspieszenie procesów transformacji cyfrowej w Wojewódzkim Szpitalu Specjalistycznym Nr 2 w Jastrzębiu-Zdroju, poprzez integrację i rozbudowę systemów informatycznych, digitalizację dokumentacji medycznej, podniesienie poziomu cyberbezpieczeństwa oraz wdrożenie rozwiązań z zakresu sztucznej inteligencji wraz z podłączeniem do Centralnego Repozytorium danych medycznych” realizowanego z Krajowego Planu Odbudowy i Zwiększania Odporności – komponentu D „Efektywność, dostępność i jakość systemu ochrony zdrowia” - inwestycji D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia.”

1. Szkolenia z zakresu cyberbezpieczeństwa dla personelu

Podniesienie poziomu bezpieczeństwa wymaga zwiększenia świadomości użytkowników systemów informatycznych. W związku z tym przewidziano szkolenia dedykowane dla personelu medycznego, administracyjnego oraz kadry kierowniczej szpitala w zakresie najlepszych praktyk cyberbezpieczeństwa. Szkolenia te mają na celu m.in. wykształcenie właściwych nawyków w pracy z systemami (np. zarządzanie hasłami, rozpoznawanie prób phishingu) oraz zapoznanie pracowników z obowiązującymi politykami bezpieczeństwa informacji.

Przedmiot zamówienia obejmuje:

- zapewnienie rocznego dostępu do platformy e-learningowej o tematyce cyberbezpieczeństwa dla maksymalnie 1000 użytkowników (podzielonych na grupy szkoleniowe po ok. 100 osób, dostosowane do różnych ról w organizacji). W ramach zamówienia Wykonawca udostępni odpowiednie materiały szkoleniowe on-line (w języku polskim, dostosowane do specyfiki sektora ochrony zdrowia) oraz będzie monitorować postępy uczestników i poziom zaliczenia przewidzianych modułów edukacyjnych. Wymaga się realizację szkoleń stacjonarnych lub webinarów uzupełniających dla wybranych grup pracowników zgodnie z zakresem wskazanym w pkt 2.

Wszystkie wymagania zamieszczone w niniejszym Opisie Przedmiotu Zamówienia są obligatoryjne.

Zamawiający nie dopuszcza zaoferowania rozwiązań wymagających dodatkowych opłat (np. ukryte koszty licencji, dopłat za certyfikaty, dopłat za dostęp do platformy).

Wykonawca przeprowadzi szkolenia stacjonarne w siedzibie Zamawiającego w terminach uzgodnionych z Zamawiającym.

2. Zakres

Przedmiotem zamówienia jest usługa przeprowadzenia szkoleń z zakresu cyberbezpieczeństwa dla kadry kierowniczej oraz personelu medycznego i administracyjnego Zamawiającego, obejmująca zagadnienia prawne, organizacyjne i techniczne dotyczące ochrony danych oraz reagowania na incydenty bezpieczeństwa, realizowana w formule warsztatowo-edukacyjnej w trybie stacjonarnym oraz online. Celem jest osiągnięcie poziomu 75% przeszkolonego personelu.

Parametr	Charakterystyka (wymagania minimalne)
Szkolenia dla kadry kierowniczej	<ul style="list-style-type: none"> Szkolenie ma na celu zwiększyć świadomość kadry kierowniczej w zakresie zrozumienia zagrożeń związanych z cyberbezpieczeństwem i podejmowania właściwych decyzji w sytuacjach kryzysowych. Szkolenie powinno obejmować następujące tematy: <ul style="list-style-type: none"> Podstawy prawne w obszarze cyberbezpieczeństwa:

	<ul style="list-style-type: none"> ○ Najważniejsze przepisy, które dotyczą każdej organizacji. ○ Odpowiedzialność kadry kierowniczej za ochronę danych i informacje. ○ Przykłady konsekwencji prawnych w przypadku naruszeń. ● Typy zagrożeń i ataków: <ul style="list-style-type: none"> ○ Socjotechnika, ○ Bezpieczeństwo poczty e-mail, ○ Bezpieczeństwo haseł, ○ Bezpieczeństwo stron internetowych. ● Reagowanie na incydenty <ul style="list-style-type: none"> ○ Co zrobić, gdy dojdzie do ataku lub wycieku danych. ○ Jak wygląda podział zadań pomiędzy zarząd, kadre kierowniczą i dział IT. ● Badania i testy bezpieczeństwa: <ul style="list-style-type: none"> ○ Dlaczego warto sprawdzać, czy systemy są bezpieczne. ○ Jak wygląda audyt bezpieczeństwa i testy praktyczne (np. sprawdzenie siły haseł, podatności stron). ○ Jak czytać raporty z badań i co z nich wynika dla kadry kierowniczej. ● Rola kadry zarządzającej: <ul style="list-style-type: none"> ○ Jak budować kulturę bezpieczeństwa w firmie.
Szkolenia dla personelu medycznego i administracyjnego	<p>Celem szkolenia jest podniesienie świadomości pracowników w zakresie bezpiecznego korzystania z systemów informatycznych i danych pacjentów, aby ograniczyć ryzyko ataków, wycieku danych czy błędów w obsłudze systemów.</p> <ul style="list-style-type: none"> ● Szkolenie powinno obejmować następujące tematy: <ul style="list-style-type: none"> ○ Socjotechnika, ○ Bezpieczeństwo poczty elektronicznej, ○ Bezpieczeństwo przeglądarek internetowych, ○ Bezpieczeństwo haseł, ○ Bezpieczeństwo urządzeń i nośników, ○ Bezpieczeństwo pracy zdalnej, ○ Incydent, ○ Odpowiedzialność prawna, ○ Podstawowych zasad cyberhigieny ○ Typów ataków wraz z przykładami ○ Reagowania na incydenty
Dodatkowe wymagania	<p>Forma:</p> <ul style="list-style-type: none"> ● Szkolenia dla kadry kierowniczej (grupa do 35 osób) <ul style="list-style-type: none"> ○ Czas trwania: 12 godzin (możliwość podziału od 2 do 4 grup szkoleniowych i szkolenie realizowane w 2 dni szkoleniowe) ○ Tryb: stacjonarnie w siedzibie Zamawiającego. ● Szkolenia dla personelu medycznego i administracyjnego odbędą się poprzez udostępnioną przez Oferenta platformę szkoleniową ● Wykonawca będzie prowadził dokumentację w postaci zestawień uczestników, którzy rozpoczęli i ukończyli szkolenie (imię, nazwisko, komórka organizacyjna, data rozpoczęcia i zakończenia szkolenia) oraz rejestru wydanych zaświadczeń. Wykonawca w ramach usługi zapewni funkcjonalność przysyłania przypomnień o konieczności ukończenia szkolenia do pracowników, którzy rozpoczęli szkolenie. Treść przypomnienia zostanie uzgodniona z Zamawiającym i będzie przesyłana raz w tygodniu. ● Wykonawca przygotuje i przekaze wszystkim uczestnikom szkolenia imienne certyfikaty/zaświadczenia o ukończeniu szkolenia

	<p>(zaświadczenie, którego wzór akceptuje Zamawiający powinno zawierać:</p> <ul style="list-style-type: none"> o temat, datę ukończenia, imię i nazwisko uczestnika szkolenia, logo Wykonawcy, oznaczenia programu KPO, logo Zamawiającego). • Zamawiający dopuszcza możliwość samodzielnego wydruku certyfikatu/zaświadczenia przez uczestnika po ukończeniu szkolenia za pośrednictwem platformy e-learningowej. • Wymagane jest przeszkolenie przynajmniej 75% pracowników pracujących na systemach informatycznych szpitala Zamawiającego (weryfikacja na podstawie list uczestników) • Kryterium odbioru w zakresie przeszkolenia 75% pracowników pracujących na systemach informatycznych szpitala uważa się za spełnione, jeżeli Wykonawca zapewnił dostęp do platformy e-learningowej dla 100% zgłoszonych osób, przeprowadził zaplanowane sesje stacjonarne/webinary oraz realizował akcję przypominającą o szkoleniach raz w tygodniu. Wykonawca nie ponosi odpowiedzialności za brak udziału pracowników w szkoleniu z przyczyn leżących po stronie Zamawiającego lub pracowników.
--	---

2.1 Zakres merytoryczny szkoleń

Zakres merytoryczny musi obejmować zagadnienia prawne, organizacyjne i techniczne, w tym wymagania dyrektywy NIS2 (Network and Information Security Directive 2 - Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii Europejskiej) oraz aktów wdrażających.

1) Moduły wspólne dla wszystkich grup

- Podstawy NIS2: zakres, rola organizacji, obowiązki i odpowiedzialność.
- Polityki wewnętrzne bezpieczeństwa informacji, zasada minimalnych uprawnień, bezpieczne hasła.
- Rozpoznawanie i zgłaszanie incydentów bezpieczeństwa (procedura wewnętrzna).
- Phishing, smishing i vishing (socjotechnika).
- Ochrona danych i prywatność - RODO (Rozporządzenie o Ochronie Danych Osobowych; ogólne rozporządzenie o ochronie danych) w kontekście cyberbezpieczeństwa.
- Bezpieczeństwo urządzeń i pracy zdalnej: VPN (Virtual Private Network - wirtualna sieć prywatna), aktualizacje, szyfrowanie, BYOD (Bring Your Own Device - korzystanie z prywatnych urządzeń do pracy).
- Bezpieczna praca z informacją: klasyfikacja, zasady udostępniania, AI (Artificial Intelligence - sztuczna inteligencja) i dane wrażliwe.

2) Kadra kierownicza / zarządzająca - moduły dodatkowe

- Odpowiedzialność kadry zarządzającej wg NIS2: nadzór, ryzyko, apetyt na ryzyko, decyzje i budżet.
- Zarządzanie incydentami: role decyzyjne, komunikacja kryzysowa, obowiązki notyfikacyjne.
- Bezpieczeństwo łańcucha dostaw i due diligence dostawców (wymogi NIS2; umowy, SLA (Service Level Agreement - umowa o gwarantowanym poziomie usług), KPI (Key Performance Indicator - kluczowy wskaźnik efektywności), audyty.
- Mierniki cyberbezpieczeństwa: ryzyko, dojrzałość, plany remediacji, przeglądy zarządcze.
- Kultura bezpieczeństwa i programy świadomościowe.

3) Personel medyczny i administracyjny - moduły dodatkowe

- Rozpoznawanie zagrożeń (phishing/socjotechnika) oraz bezpieczne linki i załączniki.
- Higiena haseł i MFA (Multi-Factor Authentication - uwierzytelnianie wieloskładnikowe); menedżery haseł; bezpieczne logowanie.
- Bezpieczne korzystanie z poczty, komunikatorów i chmury (w tym współdzielenie plików).

- Ochrona stacji roboczej i urządzeń mobilnych: aktualizacje, EDR (Endpoint Detection and Response - wykrywanie i reagowanie na incydenty na urządzeniach końcowych) / AV (Anti-Virus - oprogramowanie antywirusowe).
 - Procedura zgłaszania incydentów: dobre praktyki oraz najczęstsze błędy.
 - Bezpieczeństwo przeglądarek internetowych, urządzeń i nośników danych, odpowiedzialność prawna użytkownika.
- 4) Administratorzy IT - moduły dodatkowe
- Zarządzanie ryzykiem technicznym, hardening (utwardzanie konfiguracji), aktualizacje, kopie zapasowe i testy odtworzeniowe.
 - Zarządzanie tożsamością i dostęпами: dostępy uprzywilejowane, MFA, zasada minimalnych uprawnień, kontrola dostępu, audyt.
 - Bezpieczeństwo sieci i poczty elektronicznej.
 - Bezpieczeństwo aplikacji i API (Application Programming Interface - interfejs programowania aplikacji): SDLC (Software Development Life Cycle - cykl życia wytwarzania oprogramowania) / DevSecOps (Development, Security and Operations - podejście integrujące rozwój, bezpieczeństwo i utrzymanie), SAST (Static Application Security Testing - statyczne testy bezpieczeństwa), DAST (Dynamic Application Security Testing - dynamiczne testy bezpieczeństwa), SCA (Software Composition Analysis - analiza komponentów), SBOM (Software Bill of Materials - wykaz komponentów oprogramowania), secrets management (zarządzanie sekretami).
 - Bezpieczeństwo chmury: M365 (Microsoft 365 - pakiet usług chmurowych Microsoft) / Azure (platforma chmurowa Microsoft): konfiguracje, CSPM (Cloud Security Posture Management - zarządzanie postawą bezpieczeństwa chmury) / CIEM (Cloud Infrastructure Entitlement Management - zarządzanie uprawnieniami w chmurze), kontrola egress (kontrola ruchu wychodzącego) / DLP (Data Loss Prevention - zapobieganie utracie danych).
 - Monitoring bezpieczeństwa: XDR (Extended Detection and Response - rozszerzone wykrywanie i reagowanie), SIEM (Security Information and Event Management - zarządzanie informacjami i zdarzeniami bezpieczeństwa), SOAR (Security Orchestration, Automation and Response - orkiestracja i automatyzacja reakcji), logowanie, korelacja, retencja.
 - Reagowanie na incydenty: triage (wstępna klasyfikacja), containment (izolacja), komunikacja, dokumentacja, lessons learned (wnioski).
 - Współpraca z CSIRT (Computer Security Incident Response Team - zespół reagowania na incydenty).

2.2. Weryfikacja wiedzy i potwierdzenie ukończenia

Każde szkolenie (dla każdej grupy) zakończy się weryfikacją wiedzy w formie testu oraz wydaniem imiennego certyfikatu/zaświadczenia dla osób, które uczestniczyły w szkoleniu i spełniły wymagania zaliczenia.

- 1) Test wiedzy
- Test składa się z co najmniej 20 pytań jednokrotnego wyboru.
 - Minimalny próg zaliczenia: 80% poprawnych odpowiedzi.
 - Pytania są losowane z puli opracowanej przez Wykonawcę; pula zawiera minimum 50 różnych pytań dla każdego zestawu szkoleniowego (kadra kierownicza, personel, administratorzy IT).
 - Każdy uczestnik ma maksymalnie 5 podejść do testu.
 - Po zakończeniu testu uczestnik otrzymuje natychmiastową informację zwrotną (zestawienie poprawnych i błędnych odpowiedzi wraz ze wskazaniem prawidłowych odpowiedzi).
- 2) Certyfikat / zaświadczenie
- Dokument potwierdzający ukończenie zawiera co najmniej: imię i nazwisko uczestnika, temat szkolenia, numer dokumentu, datę ukończenia szkolenia.
 - Dodatkowo: logo Wykonawcy, logo Zamawiającego oraz oznaczenia programu KPO (Krajowy Plan Odbudowy i Zwiększania Odporności), zgodnie z wytycznymi Zamawiającego.
 - Zamawiający dopuszcza samodzielny wydruk zaświadczenia/certyfikatu przez uczestnika za pośrednictwem platformy e-learningowej.

2.3. Organizacja i czas trwania szkoleń

- Szkolenie dla kadry kierowniczej/zarządzającej realizowane jest w formie stacjonarnej i trwa co najmniej 6 godzin (nie licząc przerw).
- Szkolenie dla personelu medycznego i administracyjnego realizowane jest przede wszystkim w formie e-learningu na platformie; dopuszcza się webinaria lub sesje uzupełniające (w tym stacjonarne) w zależności od potrzeb Zamawiającego.
- Szkolenie dla administratorów IT realizowane jest jako odrębny zestaw treści na platformie e-learningowej; dopuszcza się dedykowane webinarium lub sesję warsztatową (czas łączny sesji synchronicznej wraz z testem - nie więcej niż 180 minut).

2.4. Raportowanie i wskaźniki realizacji

- Począwszy od rozpoczęcia pierwszego szkolenia Wykonawca przekazuje Zamawiającemu raz na dwa tygodnie raporty postępu: frekwencja per grupa, wskaźnik ukończeń, wskaźnik zdanych testów, ryzyko niedotrzymania KPI.
- W przypadku zagrożenia niezrealizowania kryterium odbioru Wykonawca proponuje działania naprawcze (np. dodatkowe przypomnienia, wsparcie komunikacyjne, krótkie sesje pytań i odpowiedzi, mikrolekcje).
- Po zakończeniu realizacji Wykonawca przedstawi raport końcowy: podsumowanie przebiegu, wyniki, obszary wymagające wzmocnienia oraz rekomendacje programu na kolejny rok.

2.5. Wymagania dotyczące treści i materiałów

- Treść szkoleń i materiały zostaną przygotowane w języku polskim.
- Wykonawca zapewni aktualność treści względem stanu prawnego i najlepszych praktyk na dzień realizacji; w razie zmian regulacyjnych w trakcie realizacji - zaktualizuje materiały.
- Materiały muszą być wolne od złośliwego kodu, a wszystkie linki zweryfikowane pod kątem bezpieczeństwa.
- Treść materiałów (w tym pytania testowe) Wykonawca przedstawi do akceptacji Zamawiającemu.

2.6. Prawa do materiałów

Zamawiający otrzyma prawo wewnętrznego korzystania z materiałów opracowanych w ramach zamówienia.

3. Kryteria odbioru (minimalne)

- Przeszkolenie co najmniej 75% pracowników pracujących na systemach informatycznych szpitala (weryfikacja na podstawie list/raportów z platformy), Kryterium odbioru w zakresie przeszkolenia 75% pracowników pracujących na systemach informatycznych szpitala uważa się za spełnione, jeżeli Wykonawca zapewnił dostęp do platformy e-learningowej dla 100% zgłoszonych osób, przeprowadził zaplanowane sesje stacjonarne/webinaria oraz realizował akcję przypominającą o szkoleniach raz w tygodniu. Wykonawca nie ponosi odpowiedzialności za brak udziału pracowników w szkoleniu z przyczyn leżących po stronie Zamawiającego lub pracowników.
- Przekazanie Zamawiającemu kompletu materiałów szkoleniowych oraz dokumentacji (listy uczestników, rejestr certyfikatów/zaświadczeń).
- Począwszy od momentu rozpoczęcia pierwszego szkolenia Wykonawca będzie przedstawiał Zamawiającemu raz na dwa tygodnie raportu postępu realizacji zadania (frekwencja per grupa, wskaźnik ukończeń, wskaźnik zdanych testów, ryzyko niedotrzymania KPI).
- W przypadku zagrożenia niezrealizowania kryterium odbioru, Wykonawca proponuje działania naprawcze (dodatkowe przypomnienia, wsparcie komunikacyjne, krótkie sesje Q&A, micronuggets). Zamawiający zobowiązuje się do zapewnienia wsparcia w aktywizacji pracowników do odbycia szkoleń.
- Do przygotowania materiałów szkoleń Wykonawca deleguje osoby dysponujące odpowiednią wiedzą.
- Wykonawca dostarczy rzetelny i autorski materiał szkoleniowy, bez wad i z zachowaniem należytej staranności.
- Wykonawca oświadcza legalność wykorzystania treści zewnętrznych w opracowanych materiałach szkoleniowych.

- Po zakończeniu realizacji szkoleń Wykonawca przedstawi raport końcowy, podsumowujący przebieg realizacji zadania, wyniki końcowe oraz obszary wymagające wzmocnienia i rekomendacje programowe na kolejny rok

4. Termin realizacji

Szkolenia stacjonarne (kadra kierownicza oraz ewentualne sesje uzupełniające) będą realizowane sukcesywnie, zgodnie z harmonogramem, w okresie od podpisania umowy do 29.05.2026. Dostęp do platformy e-learningowej zostanie zapewniony na okres 12 miesięcy od dnia jej uruchomienia dla Zamawiającego, przy czym uruchomienie platformy nastąpi nie później niż do dwóch tygodni po podpisaniu umowy.