

Załącznik Nr 1 do SWZ

**Samodzielny Publiczny Szpital Wojewódzki
im. Papieża Jana Pawła II w Zamościu
Al. Jana Pawła II 10
22-400 Zamość**

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Przedmiot zamówienia:

Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla personelu Zamawiającego

w ramach realizacji projektu pn.

„Rozwój usług cyfrowych i modernizacja infrastruktury informatycznej Samodzielnego
Publicznego Szpitala Wojewódzkiego im. Papieża Jana Pawła II w Zamościu”

Projekt nr KPOD.07.03-IP.10-0033/25

w ramach Krajowego Planu Odbudowy i Zwiększania Odporności

Inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez
dalszy rozwój usług cyfrowych w ochronie zdrowia”

Komponent D „Efektywność, dostępność i jakość systemu ochrony zdrowia”

Znak postępowania: DZPZ 3320.41.2026

Zamość, 10 kwietnia 2026 r.

Spis treści

Wstęp.....	3
Opis Przedmiotu Zamówienia	3
I. Szkolenia specjalistyczne dla administratorów systemów informatycznych.....	3
II. Platforma szkoleniowa.....	5
Kryteria odbioru	7

Wstęp

Zakres rzeczowy zamówienia obejmuje przeprowadzenie Szkoleń z zakresu cyberbezpieczeństwa w formie:

- a. Szkolenia specjalistyczne dla administratorów systemów informatycznych;
- b. Platforma szkoleniowa;

Opis Przedmiotu Zamówienia

I. Szkolenia specjalistyczne dla administratorów systemów informatycznych

1. Wykonawca zobowiązany jest do przeprowadzenia szkolenia specjalistycznego dla minimum 3 wskazanych przez Zamawiającego administratorów systemów informatycznych w zakresie zastosowanych oraz planowanych do zastosowania środków bezpieczeństwa.
2. Celem szkolenia jest zwiększenie kompetencji administratorów systemów informatycznych w zakresie nowych zagrożeń i sposobów zapobiegania. Przygotowanie ich do skutecznego zabezpieczania systemów informatycznych oraz zarządzania incydentami bezpieczeństwa. Szkolenie ma także za zadanie zwiększyć poziom ochrony danych oraz zapewnić zgodność z przepisami prawa przez przeszkolonych administratorów.
3. Szkolenie musi obejmować co najmniej następującą tematykę:
 - 1) Podstawy prawne krajowego systemu cyberbezpieczeństwa;
 - 2) Obowiązki wynikające z 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 (t.j. Dz. U. z 2026 poz. 20), w szczególności zapewnienie zgodności działań infrastruktury i systemów informatycznych z tymi przepisami;
 - 3) Obowiązki wynikające z Dyrektywy NIS 2 (dyrektywa (UE) 2022/2555);
 - 4) Ocenę ryzyka, w tym metody identyfikacji i analizy ryzyka związanego z infrastrukturą i systemami informatycznymi, a także środki zaradcze w celu minimalizacji ryzyka;
 - 5) Audyt wewnętrzny (cyberbezpieczeństwa) i raportowanie zgodności z przepisami;
 - 6) Zasady postępowania w razie wprowadzenia stopni alarmowych CRP dotyczących zagrożeń w cyberprzestrzeni;
 - 7) Analizę najnowszych zagrożeń cybernetycznych, takich jak ransomware, malware, phishing, ataki DDoS oraz zaawansowane uporczywe zagrożenia (Advanced Persistent Threat – APT), oszustwa i wyłudzenia z uwzględnieniem oszustwa typu Business E-mail Compromise, atak telefoniczny, spoofing, atak odwrócony – zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa i inne metody socjotechniczne;
 - 8) Rozpoznawanie i analiza wzorców ataków i technik stosowanych przez cyberprzestępców oraz sposoby ochrony;
 - 9) Identyfikację i klasyfikację incydentów bezpieczeństwa;
 - 10) Procedury przyjmowania zgłoszeń incydentów, reagowanie na incydenty;
 - 11) Sposoby szybkiego reagowania na incydenty oraz koordynacja działań naprawczych;
 - 12) Konfigurację i monitoring systemów, w tym konfigurację systemów operacyjnych i aplikacji w sposób zapewniający ich bezpieczeństwo oraz monitorowanie sieci i systemów w celu wykrywania nieautoryzowanych działań;

- 13) Bezpieczeństwo sieci, w tym konfigurację zapór sieciowych, systemów wykrywania i przeciwdziałania włamaniom (Intrusion Detection/Prevention System – IDS/IPS) oraz implementacja wirtualnych sieci prywatnych (VPN) i bezpiecznych protokołów komunikacyjnych;
 - 14) Kontrolę dostępu, w tym implementację polityk zarządzania tożsamością i dostępem (Identity Access Management – IAM) oraz konfiguracja systemów uwierzytelniania wieloskładnikowego (MFA), wady i zalety klucze sprzętowych;
 - 15) Zarządzanie uprawnieniami, w tym audyt i zarządzanie uprawnieniami użytkowników w systemach i aplikacjach. Regularna weryfikacja uprawnień i ograniczanie dostępu do niezbędnego minimum. Procedury związane z nadawaniem i odbieraniem uprawnień;
 - 16) Testy penetracyjne, w tym przeprowadzanie testów penetracyjnych, interpretacja wyników testów i wdrażanie poprawek;
 - 17) Bezpieczeństwo i ochrona danych, w tym mechanizmy ochrony danych, takie jak szyfrowanie i tworzenie kopii zapasowych. Zrozumienie zasad ochrony danych osobowych zgodnie z RODO;
 - 18) Bezpieczeństwo w chmurze, w tym bezpieczne korzystanie z usług chmurowych i zarządzanie danymi w chmurze. Zasady bezpieczeństwa specyficzne dla platform chmurowych (np. AWS, Azure, Google Cloud);
 - 19) Profilaktyka cyberbezpieczeństwa w organizacji Zamawiającego, standardy i najlepsze praktyki w tym w zakresie bezpieczeństwa urządzeń i bezpieczeństwa fizycznego;
 - 20) Sposoby podnoszenia świadomości pracowników Zamawiającego w zakresie cyberbezpieczeństwa i testowania odporności organizacji Zamawiającego na różnego rodzaju ataki;
 - 21) Umiejętność skutecznej komunikacji z zespołem, z innymi komórkami organizacji Zamawiającego i jednostek podległych oraz z interesariuszami zewnętrznymi w sprawach cyberbezpieczeństwa.
4. Szkolenia muszą obejmować dużą ilość ćwiczeń praktycznych (min. 40% czasu trwania szkolenia), pozwalających na zwiększenie kompetencji administratorów Zamawiającego związanych z:
 - 1) Zapewnieniem bezpieczeństwa przetwarzanych informacji;
 - 2) Symulacjami incydentów bezpieczeństwa;
 - 3) Analizą rzeczywistych przypadków naruszeń bezpieczeństwa;
 - 4) Zabezpieczeniem plików, poczty elektronicznej i stron WWW;
 - 5) Zabezpieczaniem sieci i serwerów;
 - 6) Zabezpieczaniem danych;
 - 7) Wykorzystywaniem zaawansowanych narzędzi informatycznych do analizy i zabezpieczania systemów informatycznych;
 - 8) Zarządzaniem w sytuacjach kryzysowych.
 5. W wyniku szkolenia administratorzy Zamawiającego muszą poznać aktualne narzędzia i metody pozwalające na poprawę bezpieczeństwa informacji, uniknięcie potencjalnego zagrożenia i zabezpieczenie ciągłości działania organizacji Zamawiającego, a w przypadku wystąpienia naruszenia – potrafić podjąć działania ograniczające skutki wystąpienia incydentu i przywrócić ciągłość działania organizacji Zamawiającego oraz zgłosić incydent do odpowiednich służb. Powinni być w pełni przygotowani do efektywnego zarządzania systemami bezpieczeństwa w organizacji oraz wdrażania najlepszych praktyk w zakresie ochrony danych i systemów informatycznych.
 6. Wykonawca zobowiązany jest do przeprowadzenia szkolenia według harmonogramu uzgodnionego między stronami w terminie 7 dni licząc od daty zawarcia umowy.
 7. Wykonawca zobowiązany jest do przeprowadzenia szkolenia w siedzibie Zamawiającego. Zamawiający zapewni stanowiska robocze dla uczestników oraz połączenie z siecią Internet.
 8. Zamawiający wymaga, aby jedna sesja szkolenia nie trwała dłużej niż 6 godzin.

9. Z przeprowadzonych szkoleń Wykonawca musi przedstawić potwierdzenie – raport z realizacji szkolenia z podpisem uczestnika.

II. Platforma szkoleniowa

1. Wykonawca udostępni Zamawiającemu platformę szkoleniową umożliwiającą przeprowadzenie szkoleń z zakresu podstaw Cyberbezpieczeństwa dla pracowników Zamawiającego, minimum 350 osób do przeszkolenia.
2. Wymagany jednoczesny dostęp dla min. 70 użytkowników.
3. Platforma musi umożliwiać użytkownikom naukę zdalną, poprzez nieprzerwany dostęp do gotowych szkoleń oraz praktyczne wykorzystanie zdobytych umiejętności za pomocą interaktywnych narzędzi i testów końcowych.
4. Platforma musi umożliwiać dostęp do min. 30 testów równocześnie dla każdego użytkownika.
5. Minimalny zakres funkcjonalności platformy szkoleniowej:
 - 1) Interfejs użytkownika: platforma musi posiadać nowoczesny, intuicyjny interfejs użytkownika.
 - 2) Materiały szkoleniowe: platforma musi oferować bibliotekę zasobów dydaktycznych, obejmując materiały w różnych formatach, takich jak dokumenty tekstowe, prezentacje, filmy wideo, animacje, quizy interaktywne oraz symulacje. Platforma musi umożliwiać aktualizację oraz rozbudowę przez wykładowców / administratorów.
 - 3) System zarządzania nauką (LMS): wymagane jest wdrożenie zaawansowanego systemu LMS, który umożliwi kompleksowe zarządzanie kursami, rejestrację i zarządzanie użytkownikami, śledzenie ich postępów i wyników w nauce, a także generowanie szczegółowych raportów dotyczących postępów i zaangażowania uczestników.
 - 4) Platforma musi umożliwiać tworzenie grup użytkowników oraz przydzielanie szkoleń dla grupy użytkowników.
 - 5) Personalizacja nauki: platforma musi umożliwiać indywidualne dostosowanie ścieżek edukacyjnych do potrzeb i preferencji każdego użytkownika, oferując funkcjonalności takie jak wybór kursów, dostosowywanie tempa nauki, indywidualne plany rozwoju oraz rekomendacje oparte na analizie postępów i zainteresowań.
 - 6) Platforma musi umożliwiać wymuszenie minimalnej ilości czasu na przyswojenie wiedzy z danego szkolenia jaką każdy z uczestników musi poświęcić na danej stronie.
 - 7) Test końcowy: każdy kurs na platformie musi mieć możliwość zakończenia testem sprawdzającym, pozwalającym na ocenę stopnia przyswojenia materiału przez uczestników. Testy muszą być zróżnicowane pod względem formy i stopnia trudności, musi być możliwość doboru losowych pytań do każdej próby zdania testu. Platforma musi umożliwiać automatyczną ocenę oraz oferować natychmiastowy wynik/ocenę dla użytkownika.
 - 8) Certyfikacja: po pomyślnym ukończeniu kursu i zaliczeniu testu końcowego, użytkownicy muszą otrzymać certyfikaty potwierdzające zdobytą wiedzę i umiejętności, możliwe do wydruku lub udostępnienia w formie cyfrowej min. PDF.
 - 9) Wykonawca zobowiązany jest do zapewnienia:
 - a. Dostępu do materiałów szkoleniowych przez okres 36 miesięcy
 - b. Raportu z realizacji szkoleń
 - 10) Platforma musi zostać dostarczona z gotowymi szkoleniami z zakresu cyberbezpieczeństwa o poniższym zakresie minimalnym:

Moduł 1: Wprowadzenie

- Czy w cyfrowym świecie naprawdę jest niebezpiecznie?
- Czym ryzykujemy zaniedbując bezpieczeństwo?
- Co zrobić, gdy popełniliśmy błąd w security?
- Co można stracić.

Moduł 2: Wiedza podstawowa

- Jak dbać o swoje stanowisko pracy
- Unikanie ryzykownego sprzętu elektronicznego
- Podstawowe oprogramowanie zabezpieczające
- Wewnętrzne szkolenia z bezpieczeństwa

Moduł 3: Jak nas podejść, popularne techniki ataków

- Socjotechnika
- Phishing
- Ransomware

Moduł 4: Jak się bronić:

- hasła, zabezpieczenie wieloczynnikowe
- antywirus
- kopie zapasowe
- aktualizacja oprogramowania
- zaufanie, a właściwie jego brak
- szyfrowanie danych

Moduł 5: Co chronimy

- osobiste dane
- Email -dlaczego należy chronić
- Przeglądarka, telefon, karty, komputer

Moduł 6: użyteczne oprogramowanie

- Samodzielne rozwijanie wiedzy o bezpieczeństwie
- Jeśli wyjdiesz z zamku, jego mury Cię nie obronią - dyscyplina
- Polityka prywatności, RODO i prawidłowe przetwarzanie danych wrażliwych

Moduł 7: Bezpieczne hasła

- Jakie hasła są naprawdę bezpieczne?
- Korzyści ze sprawdzonego narzędzia – KeePass
- Instalacja i konfiguracja KeePass
- Dodawanie i używanie własnych haseł w KeePass
- Jak współdzielić hasła firmowe za pomocą KeePass

Moduł 8: Uwierzytelnianie dwuskładnikowe

- Obrona przed wyciekiem haseł
- Czym jest uwierzytelnianie dwuskładnikowe?
- Konfiguracja uwierzytelniania dwuskładnikowego na przykładzie Google
- Konfiguracja uwierzytelniania dwuskładnikowego na przykładzie Facebook
- Do jakich usług zaleca się koniecznie korzystać z uwierzytelnienia dwuskładnikowego?

Moduł 9: Email oraz przeglądarka internetowa

- Co robimy, a co nie w przeglądarce
- Jak bezpiecznie używać poczty elektronicznej

Moduł 10: Smartfony i tablety

- Może lepiej nie korzystać ze wzoru bezpieczeństwa?
- Ile zajmuje włamywaczowi zainstalowanie szkodliwego programu na smartfonie?
- Czy można instalować aplikacje spoza sklepu google play?
- Ogranicz zaufanie do osób kontaktujących się telefonicznie

Moduł 11: Zagrożenia w pracy zdalnej

- Domownicy i własne dzieci mogą niecelowo zaszkodzić
- Jak nie dać sobie ukraść danych osobowych
- Przechwycenie tożsamości i oszuści na portalach społecznościowych

Moduł 12: Szkodliwe oprogramowanie, "robaki"

- Jak sprawdzić czy jakiś plik jest bezpieczny
- Jak poznać się, że program spowalnia komputer

Kryteria odbioru

Raport końcowy z realizacji szkoleń.