Załącznik nr 2

OPIS PRZEDMIOTU ZAMÓWIENIA

PRZEPROWADZENIE SZKOLEŃ DLA PRACOWNIKÓW W ZAKRESIE CYBERBEZPIECZEŃSTWA

Celem usługi jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników SP WZOZ MSWiA w Bydgoszczy, Projekt **„Wdrożenie e-usług w Bydgoskim Szpitalu MSWiA”** w ramach inwestycji D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia”

Zamawiający przewiduje przeprowadzenie szkolenia w następującej lokalizacji:

SP WZOZ MSWiA w Bydgoszczy
ks. R. Markwarta 4-6
85-015 Bydgoszcz

Forma szkolenia:

Szkolenie odbędzie się w formie stacjonarnej, z podziałem uczestników na grupy szkoleniowe:

1. Szkolenie dla pracowników

Szkolenie jest przeznaczone dla wszystkich pracowników Szpitala – zarówno administracyjnych, medycznych, pomocniczych, technicznych, jak i osób korzystających z systemów IT, poczty elektronicznej, urządzeń służbowych oraz przetwarzających dane pacjentów i dane organizacji.

Celem szkolenia jest podniesienie świadomości pracowników w zakresie codziennych zagrożeń cyberbezpieczeństwa oraz pokazanie, jak rozpoznawać i zgłaszać potencjalne incydenty. Szczególny nacisk zostanie położony na praktyczne sytuacje, z którymi pracownicy mogą spotkać się w codziennej pracy: fałszywe wiadomości e-mail, phishing, smishing, vishing, ransomware, podejrzane załączniki, korzystanie z haseł, praca na dokumentach, ochrona sprzętu służbowego oraz zasady bezpiecznego korzystania z systemów.

Zakres szkolenia obejmuje m.in.:

1. podstawowe zasady cyberbezpieczeństwa w codziennej pracy,
2. rolę pracownika w ochronie danych i systemów Szpitala,
3. rozpoznawanie phishingu, spoofingu, smishingu i innych form socjotechniki,
4. zasady bezpiecznego korzystania z poczty elektronicznej, internetu i systemów,
5. bezpieczne hasła i uwierzytelnianie wieloskładnikowe,
6. postępowanie z urządzeniami służbowymi, nośnikami danych i dokumentami,
7. podstawowe zasady reagowania na incydenty,
8. typów ataków wraz z przykładami
9. reagowania na incydenty
10. test wiedzy / potwierdzenie udziału w szkoleniu.

Czas trwania jednej grupy: ok. 1 godziny
Liczebność grupy: do 45 osób
Liczba grup dla około 441 pracowników: 10 grup
Rezultat: lista obecności / potwierdzenie udziału / możliwość certyfikatu uczestnictwa / materiały szkoleniowe dla każdego uczestnika (w formie papierowej lub elektronicznej)

2. Szkolenie dla zarządu i kadry kierowniczej

Szkolenie dla Dyrekcji Szpitala, kadry zarządzającej, kierowników komórek organizacyjnych, osób odpowiedzialnych za IT, bezpieczeństwo informacji, ochronę danych osobowych, jakość, administrację oraz ciągłość działania.

Celem szkolenia jest przedstawienie obowiązków kierownictwa wynikających z regulacji NIS2 oraz nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Szkolenie nie ma charakteru technicznego – jest prowadzone z perspektywy zarządczej i organizacyjnej. Jego celem jest pokazanie, co kadra kierownicza powinna rozumieć, nadzorować, dokumentować i egzekwować, aby organizacja mogła wykazać należytą staranność w obszarze cyberbezpieczeństwa.

Zakres szkolenia obejmuje m.in.:

1. obowiązki kierownictwa wynikające z NIS2 i uKSC,
2. odpowiedzialność zarządczą za system zarządzania bezpieczeństwem informacji,
3. rolę kierownictwa w nadzorze nad ryzykiem ICT i cyberbezpieczeństwa,
4. zasady zgłaszania i obsługi incydentów cyberbezpieczeństwa,
5. dokumentowanie nadzoru nad bezpieczeństwem informacji,
6. przygotowanie organizacji do audytu i kontroli,
7. przykładowe dowody audytowe, checklisty i dokumenty zarządcze,
8. praktyczne omówienie roli kadry kierowniczej w szpitalu jako podmiocie regulowanym.
9. typów ataków wraz z przykładami
10. reagowania na incydenty

Czas trwania: ok. 2 godzin
Liczebność grupy: do 45 osób
Liczba grup dla około 30 pracowników: 1 grupa
Rezultat: lista obecności / potwierdzenie udziału / możliwość certyfikatu uczestnictwa / materiały szkoleniowe dla każdego uczestnika (w formie papierowej lub elektronicznej)

Termin przeprowadzenia szkoleń:

22.06.2026 r., 24.06.2026 r., 08.07.2026 r.

Dzień	Godzina	Zakres	Grupa
Dzień 1	08:00–10:00	Obowiązki zarządu i kadry kierowniczej w świetle NIS2/uKSC Cyberbezpieczeństwo w codziennej pracy	Kadra zarządzająca
Dzień 1	10:30–11:30	Cyberbezpieczeństwo w codziennej pracy	Grupa 1
Dzień 1	12:00–13:00	Cyberbezpieczeństwo w codziennej pracy	Grupa 2
Dzień 1	13:30–14:30	Cyberbezpieczeństwo w codziennej pracy	Grupa 3

Dzień 2	09:00–10:00	Cyberbezpieczeństwo w codziennej pracy	Grupa 4
Dzień 2	10:30–11:30	Cyberbezpieczeństwo w codziennej pracy	Grupa 5
Dzień 2	12:00–13:00	Cyberbezpieczeństwo w codziennej pracy	Grupa 6
Dzień 2	13:30–14:30	Cyberbezpieczeństwo w codziennej pracy	Grupa 7
Dzień 3	09:00–10:00	Cyberbezpieczeństwo w codziennej pracy	Grupa 8
Dzień 3	10:30–11:30	Cyberbezpieczeństwo w codziennej pracy	Grupa 9
Dzień 3	12:00–13:00	Cyberbezpieczeństwo w codziennej pracy	Grupa 10
Dzień 3	13:30–14:30	Termin rezerwowy / grupa dodatkowa / uzupełnienie obecności	Rezerwa

Zamawiający dopuszcza zmianę terminów realizacji szkoleń po uzgodnieniu z Zamawiającym.