



OPIS PRZEDMIOTU ZAMÓWIENIA

1. DZIAŁANIE

Projekt	382	Fundusz Przeciwdziałania COVID-19 działań w celu do podniesienia poziomu bezpieczeństwa systemów teleinformatycznych WSS4 w Bytomiu
Postępowanie	104	Zakup sprzętu komputerowego: szkolenia z zakresu cyberbezpieczeństwa
Element	101	Opis przedmiotu zamówienia
Wersja	1	2022-10-06

2. WYMAGANIA

- Oferowane szkolenia są dostosowywane dynamicznie do słuchaczy w zależności od poziomu ich zaawansowania i zainteresowania.
- Szkolenia w zakresie cyberbezpieczeństwa skierowanych do kadry zarządzającej świadczeniodawcą oraz osób zatrudnionych u świadczeniodawcy w zakresie podstawowej świadomości bezpieczeństwa IT, w tym:
 - ochrony przed zaawansowanymi atakami przez pocztę i WWW,
 - Rodzaje ataków mailowych: phishing, spearphishing, Sexstortion Scams, malware itp.
 - Rodzaje ataków przez WWW: Atak „przynęta z zamianą”, Podszywanie się pod DNS, Cross-Server Attack, Spoofing itp.
 - Inne: SMS phishing, fałszywe aplikacje
 - Jak rozpoznawać ataki? Jak się zabezpieczać?
 - tworzenia i zarządzania polityką haseł i tożsamości,
 - Jak powinny być tworzone bezpieczne hasła?
 - Czy standardowe hasło (8 znaków) zmieniane co 30 dni jest bezpieczne? ... i dlaczego nie.
 - Jakie są alternatywne metody zabezpieczania swojej tożsamości i poświadczeń do logowania?
 - zarządzania ryzykiem, dokumentacją i polityką bezpieczeństwa w jednostkach publicznych w świetle rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 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 2017 r. poz. 2247),
 - Na czym polega zarządzanie ryzykiem?
 - Co to jest Polityka Bezpieczeństwa, czemu służy i co powinna zawierać
 - Czy Polityka Bezpieczeństwa wystarcza? Jakie dokumenty należy jeszcze posiadać w organizacji.
 - wykonywania kopii zapasowych oraz tworzenia i utrzymania polityki ciągłości działania.
 - Dobre praktyki w zakresie wykonywania kopii bezpieczeństwa.
 - Co to jest RTO i RPO i czemu są niezbędne dla prawidłowego sporządzania kopii?
 - Polityka Ciągłości Działania – Czym się różni od Polityki Bezpieczeństwa? Co powinna zawierać?
- Szkolenia odbywać się będą w grupach max. 25 osobowych w siedzibie Zamawiającego. Zamawiający na czas szkoleń nieodpłatnie użyczy salę. Nie uznaje się szkoleń przez platformę. Szkolenie w miejscu i czasie wyznaczonym przez Zamawiającego. Posiadanie wyposażenia multimedialnego po stronie Wykonawcy
- Zamawiający w porozumieniu z Wykonawcą ustali terminarz szkoleń w poszczególnych grupach szkoleniowych,
- Szkolenia będą prowadzone w dniach roboczych (od poniedziałku do piątku) w godzinach od 800 do 1400,
- Szkolenia muszą być prowadzone przez wykwalifikowaną kadrę dydaktyczną, znającą specyfikę i tematykę szkolenia,
- Preferowane formy szkolenia; wykłady w oparciu o dostarczone przez wykonawcę materiały
- Wykonawca sporządzi pełną dokumentację szkolenia, zgodną z obowiązującymi przepisami, którą będzie przechowywał w swojej siedzibie przez okres co najmniej 5 lat od zakończenia szkolenia,
- Szkolenie musi być zakończone wydaniem zaświadczenia zgodnych z obowiązującymi przepisami,
- Wykonawca przekazuje zamawiającemu kopie rejestru wydanych zaświadczeń,
- Na dzień roku należy przeszkolić następującą ilość pracowników:

Lp.	Grupa pracowników	Minimalny czas trwania szkolenia (godzin zegarowe)	Ilość pracowników podlegających szkoleniu
1.	Dyrekcja WSS4 W Bytomiu	2 godziny zegarowe-120minut	3
2.	Naczelnia Pielęgniarka		1
3.	Dział Księgowości		15
4.	Dział Administracji		7
5.	Dział Techniczny		3
6.	Dział Kadr		7
7.	Dział Zamówień Publicznych		3
8.	Pozostali pracownicy części techniczno-administracyjnej		16
9.	Sekcja Aparatury		2
10.	Sekretarki medyczne		21
11.	Pielęgniarki Oddziałowe	2 godziny zegarowe-120minut	17
12.	Kierownicy Oddziałów		14
13.	Sekcja Informatyki	4 godziny zegarowe-240 minut	4
14.	Rejestracja	2 godziny zegarowe-120minut	8
15.	Call center		4
RAZEM			125