**Załącznik nr 2 – Opis przedmiotu zamówienia**

**Piekary 31.08.2023**

**„Szkolenia w zakresie cyberbezpieczeństwa skierowanych do kadry zarządzającej świadczeniodawcą oraz osób zatrudnionych w SP Wojewódzkim Szpitalu Chirurgii Urazowej im. dr. Janusza Daaba w Piekarach Śląskich”**

**WYMAGANIA**

1. Oferowane szkolenia są dostosowywane dynamicznie do słuchaczy w zależności od poziomu ich zaawansowania i zainteresowania.

2. Szkolenia w zakresie cyberbezpieczeństwa skierowanych do kadry zarządzającej świadczeniodawcą oraz osób zatrudnionych u świadczeniodawcy w zakresie podstawowej świadomości bezpieczeństwa IT, minimum:

* Socjotechnika – wstęp teoretyczny mający zapoznać użytkownika z podstawowymi pojęciami i nomenklaturą stosowaną w cyberbezpieczeństwie na poziomie technik inżynierii społecznej.
* Bezpieczeństwo poczty e-mail – prezentacja form i przykładów ataków ukierunkowanych na użytkownika końcowego z wykorzystaniem wiadomości e-mail (phishing, spearphishing) oraz metod weryfikacji i działań zapobiegawczych,
* Bezpieczeństwo przeglądarek internetowych – przekazanie najważniejszych zasad bezpieczeństwa podczas korzystania z przeglądarek wraz z zwróceniem szczególnej uwagi na sposoby weryfikacji poprawności adresów www i połączeń szyfrowanych,
* Bezpieczeństwo haseł – przegląd najczęstszych błędów popełnianych przy tworzeniu haseł   
  i zapoznanie z najlepszymi praktykami dotyczącymi polityk autoryzacji i uwierzytelniania oraz metodami generowania silnych haseł,
* Bezpieczeństwo pracy zdalnej – porady dotyczące bezpiecznego korzystania z domowej sieci wi-fi, czy korzystania ze sprzętu służbowego poza firmą. Poruszane są także tematy połączenia VPN, polityk dotyczących korzystania z prywatnego sprzętu do zadań służbowych, a także sposoby na uniknięcie wycieków wrażliwych danych,
* Bezpieczeństwo urządzeń i nośników – omówienie tematu szyfrowania dysków przenośnych, czy polityk firmy w przypadkach zgubienia lub kradzieży sprzętu. Demonstracja i objaśnienie możliwych skutków podłączania nieznanych nośników danych do komputerów służbowych,
* Bezpieczeństwo urządzeń mobilnych – prezentacja zagrożeń oraz metod obrony związanych   
  z użytkowaniem telefonów komórkowych i smartfonów (smishing, vishing, złośliwe kody QR, oszustwa na Blik itp.)
* Polityka czystego biurka – dyskusja na temat czynności i procedur mających na celu ochronę poufnych danych,
* Incydent – uczestnik podczas omawiania prezentowanych metod ataków socjotechnicznych zapoznawany jest z autentycznymi przykładami incydentów. Każda przytoczona sytuacja zostaje szczegółowo omówiona od źródła, poprzez przebieg do skutków jakie spowodowała. Przedyskutowane zostają również prawidłowe reakcje na atak i sposoby obrony.

3. 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

4. Zamawiający w porozumieniu z Wykonawcą ustali terminarz szkoleń w poszczególnych grupach szkoleniowych,

5. Szkolenia będą prowadzone w dniach roboczych (od poniedziałku do piątku) w godzinach od 8.00 do 14.00,

6. Szkolenia muszą być prowadzone przez wykwalifikowaną kadrę dydaktyczną, znającą specyfikę i tematykę szkolenia,

7. Preferowane formy szkolenia; wykłady w oparciu o dostarczone przez wykonawcę materiały, ćwiczenia praktyczne

8. Wykonawca przechowuje dokumentację ze szkolenia niezbędną do wykazania jego odbycia, zgodną z obowiązującymi przepisami.

9. Szkolenie musi być zakończone wydaniem zaświadczenia zgodnych z obowiązującymi przepisami,

10. Wykonawca przekaże zamawiającemu imienne zaświadczenia z odbytych szkoleń oraz kopie rejestru wydanych zaświadczeń,

11. Czas szkolenia przewidziano na 120 minut.

**Zamawiający przewiduje szkolenie dla 100 osób**

Czas realizacji zamówienia: zakończenie szkoleń do 26 września 2023