Załącznik nr 3b

OPIS PRZEDMIOTU ZAMÓWIENIA

PAKIET NR 2

Przedmiotem zamówienia jest szkolenie dot. cyberbezpieczeństwa wykonane na potrzeby i na podstawie „ZARZĄDZENIE NR 117/2022/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA z dnia 20 września 2022 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców".

Szkolenie może być przeprowadzone przez firmę posiadającą niezbędne kwalifikacje, specjalistyczną wiedzę oraz właściwe doświadczenie w zakresie analizy poziomu cyberbezpieczeństwa systemów teleinformatycznych.

1) Szkolenie będzie przeznaczone dla 225 osób. Szkolenie odbędzie się poprzez dedykowaną platformę szkoleniową udostępnioną przez Wykonawcę.
2) Szkolenie zostanie przeprowadzone z uwzględnieniem faktu, że uczestnicy szkolenia mogą nie posiadać wiedzy informatycznej i technicznej.
3) Wykonawca przygotuje dla zamawiającego materiały ze szkolenia, które będzie mógł wykorzystać do przeszkolenia nieobecnych lub nowych pracowników. Szkolenie będzie udostępniane pracownikom Zamawiającego **przez okres 12 miesięcy** od momentu rozpoczęcia szkoleń.
4) Szkolenie ma na celu uświadomić pracownikom niebezpieczeństwa w cyberprzestrzeni zarówno w pracy jak i w życiu prywatnym. Agenda szkolenia powinna obejmować m.in. następujące zagadnienia:

Zakres ogólny/podstawowy:

- Czym jest cyberbezpieczeństwo?
- Metody nieautoryzowanego pozyskania danych + przykłady
- Zagrożenia w sieci (w tym phishing, ransomware, malware, socjotechnika, atak telefoniczny, spoofing, atak odwrócony - zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa) + przykłady
- Bezpiecznie przetwarzanie danych: szyfrowanie, przechowywanie, udostępnianie, komunikacja
- Bezpieczne hasła, managery haseł, autoryzacja dwuetapowa, klucze sprzętowe
- Metody obrony oraz przeciwdziałania (w tym: przed wyłudzeniem danych osobowych za pomocą metod socjotechnicznych, programowaniem mogącym zablokować dostęp do urządzeń firmowych, szkodliwymi programami mogącymi pozyskać dane firmowe lub osobiste
- Bezpieczne korzystanie z mediów społecznościowych
- Bezpieczne korzystanie ze smartfonów
- Wskazanie miejsc organizacji, oraz informacji, które należy chronić, by zniwelować ryzyko narażenia firmy na straty finansowe.
- Wskazanie zasad cyberhigieny

Kontekst danych medycznych:

- Dane medyczne i osobowe – przetwarzanie
- Zasady postępowania z danymi szczególnie wrażliwymi
- Zgłaszanie incydentów dot. danych medycznych i osobowych
- Przykłady ataków hackerskich na szpitale

5) W ramach zamówienia dostarczone zostaną także testy sprawdzające wiedzę po szkoleniu składające się z przynajmniej 15 pytań z zakresów wymienionych w pkt. 2.
6) W ramach szkolenia zostaną zorganizowane konsultacje z kadrą zarządzającą. Tematem dyskusji będzie kontekst cyberbezpieczeństwa i prewencji w jednostkach ochrony zdrowia oraz tematyka 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).