**Załącznik nr 1 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

# Zakres przedmiotu zamówienia

Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa oraz kampanii cyberawereness z zakresu cyberbezpieczeństwa. Program szkoleniowy (zwany dalej w skrócie „programem”) przedmiotowego zamówienia obejmuje działania edukacyjne prowadzone w kilku komplementarnych formatach, dostosowanych do specyfiki i potrzeb poszczególnych grup pracowników Urzędu Zamówień Publicznych oraz Krajowej Izby Odwoławczej. Cykl szkoleniowy łączy bloki wspólne dla wszystkich oraz dedykowane moduły dla grup funkcyjnych. W całym cyklu szkoleniowym Wykonawca omówi tematy: najpopularniejsze zagrożenia, phishing, socjotechnika, incydenty bezpieczeństwa, złośliwe oprogramowanie, higiena cyfrowa, bezpieczeństwo poczty elektronicznej, bezpieczeństwo urządzeń przenośnych, MFA, ślady cyfrowe, ochrona danych osobowych, praca zdalna, bezpieczeństwo nośników, OSINT, ransomware, polityka haseł, bezpieczeństwo w mediach społecznościowych, praktyczne ćwiczenia i symulacje ataków. Dedykowane bloki tematyczne w ramach szkoleń stacjonarnych i szkoleń online uwzględniać mają specyfikę pracy, typowe zagrożenia oraz praktyczne aspekty bezpieczeństwa.

## Zakres rzeczowy – podział na komponenty

### 1.1.1. Szkolenia stacjonarne

* Realizacja szkoleń stacjonarnych obejmuje dwa cykle szkoleniowe (po 4 szkolenia) dla w sumie maksymalnie 160 osób w grupach do 40 osób. Część merytoryczna (czyli nie uwzględniając kwestii organizacyjnych, powitania i innych elementów nieodnoszących się do tematu danego szkolenia) jednego szkolenia trwa 45 minut.
* Zamawiający dopuszcza przeprowadzenie w jednym dniu maksymalnie dwóch szkoleń
* Zamawiający nie dopuszcza przeprowadzenia obu cykli szkoleniowych tego samego dnia
* Szkolenia stacjonarne odbędą się w siedzibie Zamawiającego w Warszawie przy ul. Postępu 17a, w sali zapewnionej przez Zamawiającego.
* Pierwszy cykl szkoleń ma obejmować swoim zakresem kluczowe tematy dotyczące cyberbezpieczeństwa przedstawione w punkcie 1., a drugi cykl bezpieczną pracę grupową na Teams.
* Zamawiający odpowiada za wyposażenie sali (rzutnik multimedialny, flipchart, flamastry).
* Za nabór uczestników szkoleń odpowiada Zamawiający.
* Materiały na szkolenie przygotowuje Wykonawca.
* Wykonawca dostarczy osobom biorącym udział w szkoleniu zaświadczenia uczestnictwa

### 1.1.2. Szkolenia zdalne

* Tematyka szkoleń będzie obejmować kluczowe tematy dotyczące cyberbezpieczeństwa przedstawione w punkcie 1., wzbogacone o ich pogłębienie oraz omówienie przykładów;
* Realizacja szkoleń zdalnych odbędzie się na platformie MS Teams Zamawiającego, z możliwością zadawania pytań na żywo, nagrywane i archiwizowane przez zamawiającego.
* Zamawiający przewiduje wykorzystanie nagrań do szkolenia nowych pracowników.
* Zamawiający przewiduje 10 szkoleń w trakcie realizacji umowy, każde trwające 60 minut, w terminach uzgodnionych z Wykonawcą.
* Każde ze szkoleń ma odbyć się w innym terminie, a harmonogram zostanie uzgodniony po podpisaniu umowy.
* Materiały na szkolenie przygotowuje Wykonawca.

1.1.3. Materiał dla pracowników

* Wykonawca przygotuje przewodnik po bezpieczeństwie (3 strony, elektronicznie). Jego zakres obejmuje aktualne strategie ataków cyber, sposoby rozpoznania zagrożeń oraz omówienie zasad zgłaszania incydentów obowiązujących w urzędzie.

### 1.1.4. OSINT

Wykonawca zobowiązany jest do przeprowadzenia OSINT podstawowego dla 17 osób i rozszerzonego dla 5 osób.

### 1.1.5. Szkolenia indywidualne dla kierownictwa i dyrektorów

* **Kierownictwo (5 osób)**: Szkolenia indywidualne 1:1 (stacjonarne w siedzibie Zamawiającego), trwające 45–60 minut, przygotowane na podstawie OSINT rozszerzonego, z czasem na pytania indywidualne. Zakres spotkania obejmuje przekrojowe zagadnienia opisane w punkcie 1., analizę indywidualnych zagrożeń, odpowiedzialność prawną i organizacyjną, zarządzanie ryzykiem oraz wdrażanie kultury bezpieczeństwa, zastosowanie kluczy U2F w trakcie realizacji zadań służbowych.
* **Dyrektorzy (17 osób)**: Szkolenia indywidualne 1:1 (stacjonarne w siedzibie Zamawiającego), 45–60 minut, przygotowane na podstawie OSINT podstawowego, Zakres spotkania obejmuje przekrojowe zagadnienia opisane w punkcie 1. z naciskiem na praktyczne aspekty zarządzania ryzykiem, ochronę danych i komunikację w zespole, zastosowanie kluczy U2F w trakcie realizacji zadań służbowych.
* Szkolenia nie są dokumentowane, nie przewiduje się przekazywania materiałów podsumowujących.

### 1.1.6. Kampania cyberawareness

* W ramach programu szkoleniowego realizowana będzie kampania cyber awareness (zwana dalej w skrócie „kampanią”), której celem jest praktyczne wzmacnianie odporności pracowników Urzędu Zamówień Publicznych na ataki socjotechniczne oraz utrwalanie nawyków bezpiecznego zachowania. Pozwoli to na weryfikację zdobytej w trakcie szkoleń wiedzy i weryfikację jej w czasie działań. W ramach kampanii przeprowadzane będą działania phishingowe, które mają weryfikować skuteczność szkoleń i umożliwią opracowanie tematów kolejnych szkoleń dla pracowników realizowanych w trakcie trwania umowy.
* Wykonawca przeprowadzi następujące działania w ramach kampanii cyber awareness: 2x phishing do 200 osób, 2x smishing do maks. 20 osób, 2x podrzucenie pendrive w siedzibie Zamawiającego oraz vishing do 3 osób.
* Działania prowadzone w ramach kampanii mogą być mieszane po uzgodnieniu z  Zamawiającym.
* W ramach kampanii prowadzone będą działania dotyczące SMS – kierowane do wąskiej grupy osób. Zakres i scenariusz kampanii zostaną uzgodniony w trakcie realizacji umowy.
* W ramach kampanii prowadzone będą działania telefoniczne – vishing do trzech ustalonych indywidualnie osób funkcyjnych wskazanych przez Zamawiającego na etapie realizacji umowy. Zakres i scenariusz kampanii zostaną uzgodniony w trakcie realizacji umowy. W ramach realizacji zadania Wykonawca podejmie każdorazowo maksymalnie trzy próby dodzwonienia się w terminach uzgodnionych z Zamawiającym.
* Szablony wiadomości każdorazowo zatwierdzane przez zamawiającego.
* Zamawiający wymaga realizacji usługi w dni robocze w godzinach 8:00 – 15:00 według harmonogramów opracowanych przez Wykonawcę w uzgodnieniu z Zamawiającym.
* Wykonawca opracuje Raporty z kampanii zawierające szczegółową analizę skuteczności szablonów, statystyki uczestnictwa, rekomendacje naprawcze dla grup z niskim zaangażowaniem oraz przeprowadzi każdorazowo konsultacje z zespołem ds. Bezpieczeństwa po stronie Zamawiającego.
* Kampanie mają być prowadzone z różnych domen, a telefoniczne/sms z różnych numerów.
* Zamawiający zapewni integrację z Microsoft Entra ID na potrzeby przeprowadzenia kampanii.

### 1.1.7. Konsultacje

* Przewidziane są okresowe konsultacje/przeglądy programu szkoleń, których celem jest omówienie postępów, wyników raportowania oraz rekomendacji dotyczących dalszych działań edukacyjnych.
* Wszelka komunikacja prowadzona jest drogą elektroniczną (e-mail), a w przypadku konsultacji – również w formie wideokonferencji.
* Zamawiający przewiduje łącznie 10 h konsultacji w trakcie trwania umowy.

### 1.1.8. Raporty cząstkowe i Raport zamknięcia

* Po każdej kampanii wykonawca przygotowuje Raport cząstkowy zawierający: opis przeprowadzonej kampanii wraz z jej scenariuszem, szczegółową analizę jej skuteczności poszczególnych szablonów ataków, statystyki liczby użytkowników, którzy nie wzięli udziału w kampanii, statystyki uczestnictwa, podsumowanie i wnioski.
* Raporty cząstkowe będą każdorazowo konsultowane z zespołem ds. bezpieczeństwa zamawiającego po każdej kampanii (forma konsultacji elastyczna: spotkanie online, raport pisemny lub inna uzgodniona).
* Raport zamknięcia będzie zawierał opis wszystkich, przeprowadzonych szkoleń grupowych oraz indywidualnych przeprowadzonej kampanii, wraz z podsumowaniem, komentarzem eksperckim oraz wnioskami i zaleceniami dla Zamawiającego.

### 1.2. Minimalne wymagania dotyczące OSINT

* W zakresie OSINT podstawowy Wykonawca powinien przeszukać rejestry publiczne (REGON, CEIDG, KRS), portale społecznościowe (Facebook, Instagram, LinkedIn).
* W zakresie OSINT rozszerzony, Wykonawca realizuje zakres OSINT podstawowy oraz przeszukuje zasoby tzw. „darkweb” (wycieki haseł, tematy dyskusyjne na temat osoby) – na podstawie adresu email służbowego i prywatnego.
* Pozyskany materiał stanowi informacje poufne. Wykonawca zapewnia, że informacje te będą znane wyłącznie pracownikowi wykonującego OSINT oraz osobie, z którą planowane jest spotkanie.

### 1.3. Organizacja i komunikacja

* Komunikacja dotycząca terminów szkoleń prowadzona jest przez Zamawiającego.
* Szkolenia mogą być nagrywane na platformie MS Teams zamawiającego, za zgodą uczestników; Wykonawca wyraża zgodę na utrwalenie wizerunku.
* Materiały szkoleniowe przygotowuje Wykonawca dla wszystkich szkoleń.
* Wykonawca prowadzi statystyki liczby przeprowadzonych szkoleń kwartalnie i na koniec umowy.

# Mierzenie efektywności programu

## Wskaźniki efektywności (KPI)

Efektywność programu będzie monitorowana na bieżąco za pomocą raportów eksperckich przygotowanych przez Wykonawcę. Główne KPI obejmują:

* **Phishing Failure Rate** – odsetek użytkowników, którzy dali się złapać na symulowany phishing (kliknięcie, podanie danych).
* **Phishing Report Rate** – odsetek użytkowników, którzy prawidłowo zgłosili podejrzaną wiadomość.
* **Liczba użytkowników niebiorących udziału w kampaniach** – monitorowanie i raportowanie wskaźników również dla użytkowników, którzy nie wzięli udziału w kampanii phishingowej.

Wskaźniki będą raportowane ogólnie oraz w segmentacji użytkowników (wg działów, ról) w raportach i kampaniach.

## Sposób pomiaru, raportowania i ewaluacji

* **Pomiar bazowy:** Przed rozpoczęciem programu Wykonawca przeprowadzi symulację phishingu. Średnia z efektów symulacji osiągniętych przez Wykonawcę oraz efekty osiągnięte przez Zamawiającego przy realizacji symulacji phishingu skierowanej do wszystkich pracowników, stanowić będą poziom wyjściowy odporności (% kliknięć w link oraz % podania danych logowania). Dodatkowym wskaźnikiem nie mierzonym wcześniej będzie % zgłoszeń podejrzanej treści.
* **Archiwizacja:** Raporty i rekomendacje przekazywane zamawiającemu po każdej kampanii, bez konieczności prowadzenia archiwum przez Wykonawcę.

## 2.3. Raportowanie i analityka cyber awareness i symulacje ataków

* Po każdej kampanii wykonawca przygotowuje raport zawierający: szczegółową analizę skuteczności poszczególnych szablonów ataków (np. które szablony były najskuteczniejsze), statystyki liczby użytkowników, którzy nie wzięli udziału w kampanii, statystyki uczestnictwa,
* Wykonawca przestawi rekomendacje eksperckie dotyczące konkretnych działań naprawczych dla grup z niskim zaangażowaniem.

Raporty będą każdorazowo konsultowane z zespołem ds. bezpieczeństwa zamawiającego po każdej kampanii (forma konsultacji elastyczna: spotkanie online, raport pisemny lub inna uzgodniona).

# 3. Wymagania formalne i zgodność

## 3.1. Oznaczenia materiałów i dokumentów

Wszystkie materiały, dokumenty i efekty pracy muszą być oznaczone zgodnie z wymogami Księgi Identyfikacji Wizualnej KPO oraz zawierać informację o finansowaniu ze środków KPO i NextGenerationEU. Zamawiający udostępni wzory oznaczeń i logotypów. Wykonawca zobowiązany jest do stosowania się do wytycznych dotyczących komunikacji i promocji projektu, w tym do przygotowania materiałów komunikacyjnych do kampanii wewnętrznej. Dokumentacja dostępna jest na stronie <https://www.kpo.gov.pl/strony/o-kpo/dla-instytucji/dokumenty/strategia-promocji-i-informacji-kpo/>

Wszelkie dokumenty wytworzenie w trakcie realizacji przedmiotu zamówienia będą wytworzone tylko w formie elektronicznej[[1]](#footnote-1). Nie dopuszcza się formy papierowej.

## 3.2. Zasady przetwarzania i usuwania danych

Wszystkie dane osobowe muszą być przetwarzane zgodnie z RODO/GDPR. Przetwarzanie i retencja danych odbywają się wyłącznie w regionie UE/EOG.

### 3.2.1. Retencja i archiwizacja danych

Nie przewiduje się szczególnych wymagań dotyczących archiwizacji i retencji danych po zakończeniu projektu poza okresem przejściowym uzgodnionym w umowie.

## 3.3. Wymagania dotyczące języka i formatu materiałów

Materiały szkoleniowe, komunikaty i raporty przygotowywane są w języku polskim. Formaty plików materiałów, w których mają być one przygotowane to np.: PDF, DOCX lub PPTX.

1. Aspekt środowiskowy. [↑](#footnote-ref-1)