



Cyberbezpieczny Samorząd

Załącznik nr 2

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest przeprowadzenie 5-cio dniowego szkolenia dla pracowników Zamawiającego w zakresie cyberbezpieczeństwa, dotyczącego praktycznego stosowania mechanizmów bezpieczeństwa korespondencji i zabezpieczania danych, w ramach projektu konkursu grantowego pn. „Cyberbezpieczny Samorząd” realizowanego z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Priorytet II: Zaawansowane usługi cyfrowe (dalej: konkurs „Cyberbezpieczny Samorząd”).
2. Szkolenie powinno składać się z części teoretycznej i praktycznej.
3. Szczegółowy zakres szkolenia teoretycznego powinien obejmować co najmniej następujące zagadnienia:
 - 3.1. Wprowadzenie do bezpieczeństwa cyfrowego w organizacji
 - Omówienie zakresu niebezpieczeństw cybernetycznych, którym najczęściej poddane są instytucje administracji publicznej i samorządowej.
 - Przegląd najczęstszych form ataków i ich konsekwencji dla instytucji administracji publicznej, w tym samorządowej oraz metod zmniejszania potencjalnego ryzyka w realizacji bieżących zadań - na przykładach z ostatnich 6 m-cy.
 - 3.2. Cyfrowe bezpieczeństwo fizyczne. Podstawowe zasady bezpieczeństwa fizycznego w kontekście możliwych ataków cyfrowych:
 - Dostęp do obiektu instytucji administracji publicznej i samorządowej (ataki hackerskie typu "tailgating" i inne formy wejść i zagrożeń fizycznych).
 - Zapewnienie bezpieczeństwa fizycznego dla dokumentów fizycznie umieszczonych w budynku instytucji.
 - Dostęp fizyczny do sprzętu i oprogramowania IT w firmie, w tym zewnętrzne nośniki pamięci cyfrowej.
 - 3.3. Cyberbezpieczeństwo:
 - Podstawowe zasady higieny i bezpieczeństwa cyfrowego w jednostce administracji publicznej i samorządowej na przykładach: ataki wykorzystujące inżynierię społeczną, ataki złośliwym oprogramowaniem, próby wyłudzenia danych.
 - Korzystanie z poczty elektronicznej - szyfrowanie danych, budowanie bezpiecznych haseł, zagrożenie przejęcia poczty firmowej i prywatnej, możliwe symptomy infekcji komputera.
 - Uwierzytelnianie dwuskładnikowe - powody, metody, narzędzia.
 - Metody zmniejszania potencjalnego ryzyka w realizacji bieżących zadań.
 - Komunikacja kryzysowa – co należy zrobić w przypadku wystąpienia incydentu.
 - 3.4. Bezpieczeństwo danych instytucji administracji publicznej i samorządowej – czynnik ludzki:





Cyberbezpieczny Samorząd

- Rozmowy o pracy w miejscach publicznych – zasady bezpiecznych rozmów, czego unikać, jak ograniczyć ryzyko.
 - Udostępnianie zewnętrzne – zasady kwalifikacji, przesyłanie danych e-mailem, przenoszenie na pendriv-ie, korzystanie z nośników reklamowych, wykorzystanie folderów dzielonych i tymczasowych, szyfrowanie.
 - Makra – wykorzystanie do ataków, kiedy włączać makra, jak unikać zagrożeń.
 - Usuwanie danych – jak zadbać o dane, jak przechowywać dane, miejsca przechowywania danych.
 - RODO – podstawowe wymagania, jak działać zgodnie z RODO, na co zwracać uwagę w codziennej pracy.
- 3.5. Bezpieczna praca z przeglądarką:
- Strony szyfrowane – jak rozpoznać strony szyfrowane i nieszyfrowane, co mówi nam oznaczenie https i kłódka, jak sprawdzić, czy strona jest bezpieczna, pułapki https, nowe oznaczenia szyfrowania.
 - Certyfikaty – co oznacza SSL, jak sprawdzić certyfikat strony, na co zwrócić uwagę.
- 3.6. Prywatne działania w sieci i ekspozycja na zagrożenia cyfrowe instytucji publicznej i samorządowej:
- Zagrożenia związane z używaniem poczty prywatnej do celów służbowych.
 - Potencjalne konsekwencje dla Urzędu wynikające z przejęcia prywatnego konta pracownika na portalu społecznościowym.
 - Zagrożenia wykorzystywania służbowych urządzeń mobilnych do celów prywatnych.
 - Bezpieczeństwo psychiczne w używaniu portali społecznościowych.
 - Wykorzystanie sztucznej inteligencji do ataków socjotechnicznych.
- 3.7. Sprzęt firmowy, praca zdalna:
- Na co warto zwrócić uwagę w kontekście bezpieczeństwa, pracując z domu lub w podróży.
4. Oprócz szkolenia teoretycznego Wykonawca powinien zrealizować ćwiczenia praktyczne obejmujące tematykę szkolenia (np. w formie QiuZ/gry lub ćwiczenia).
5. Wykonawca zobowiązany jest przeprowadzić testy sprawdzające wiedzę – na wstępie szkolenia i na jego zakończeniu. Po zakończeniu szkolenia, zostanie udostępniona ankieta ewaluacyjna szkolenia, a wynik ankiety w formie raportu zostanie przekazany Zamawiającemu.
6. Dokumentowanie prowadzonych zajęć i działań nastąpi poprzez prowadzenie list obecności, na drukach oznaczonych logotypami, przygotowanych przez Zamawiającego. Listy obecności zostaną przekazane Zamawiającemu niezwłocznie po przeprowadzeniu szkolenia.
7. Wykonawca jest zobowiązany w terminie do 7 dni kalendarzowych po zakończeniu realizacji Przedmiotu zamówienia dostarczyć certyfikaty ukończenia szkolenia, zgodnie z listą obecności.





Cyberbezpieczny Samorząd

8. Zamawiający wskazuje jako miejsce przeprowadzenia szkolenia siedzibę Zamawiającego lub inną lokalizację wskazaną przez Zamawiającego w odległości do 10 km od siedziby Zamawiającego. Rezerwacja miejsca prowadzenia zajęć jest po stronie i na koszt Zamawiającego.
9. Ekran odpowiedniej wielkości lub rzutnik będzie udostępniony przez Zamawiającego. Zamawiający zapewni również dostęp do energii elektrycznej (gniazdko).
10. W szkoleniu będzie brało udział około 52 osób.
11. Wykonawca zobowiązuje się w terminie 7 dni od dnia podpisania umowy dostarczyć Zamawiającemu:
 - 1) proponowane terminy szkolenia;
 - 2) szczegółowy zakres merytoryczny szkolenia;
 - 3) dzienny harmonogram szkolenia.

Wykonawca zobowiązany jest do współpracy i konsultacji z Zamawiającym oraz do wprowadzania poprawek w sporządzanej przez siebie dokumentacji zgodnie z sugestiami Zamawiającego na każdym etapie realizacji zamówienia. Szkolenia będą przeprowadzone po ostatecznej akceptacji dokumentacji przez Zamawiającego.

12. W ramach organizacji szkolenia Wykonawca zapewni:
 - 1) materiały szkoleniowe, obejmujące szczegółowy zakres merytoryczny szkolenia i harmonogram dzienny szkolenia (materiały zostaną przekazane każdemu uczestnikowi szkolenia w wersji elektronicznej – nieodpłatnie, na własność);
 - 2) oznakowanie w odpowiedni sposób materiałów szkoleniowych przekazanych uczestnikom (zgodnie z zasadami określony w konkursie „Cyberbezpieczny Samorząd”;
 - 3) wydanie Zamawiającemu szkolenia zaświadczeń/certyfikatu o ukończeniu szkolenia dla każdego uczestnika;
 - 4) kadrę trenerską posiadającą wiedzę, doświadczenie i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkolenia;

