

OPIS PRZEDMIOTU ZAMÓWIENIA

„Przeprowadzenie szkoleń w ramach projektu pn. „Cyberbezpieczny Samorząd – Miasto Będzin” współfinansowanego przez Unię Europejską z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa”, w ramach Konkursu grantowego „Cyberbezpieczny Samorząd”

Celem realizacji szkoleń jest podniesienie świadomości i umiejętności praktycznych kadr jednostek krajowego systemu cyberbezpieczeństwa o cyberbezpieczeństwie, obowiązkach wynikających z Ustawy o krajowym systemie cyberbezpieczeństwa oraz stosowanych standardach i dobrych praktykach w organizacjach.

Szkolenie pracowników Urzędu Miejskiego w Będzinie, ma w swoim nadrzędnym założeniu nauczyć kadrę zasad postępowania w razie ataku oraz schematu funkcjonowania, w sytuacji wystąpienia różnych rodzajów ataków, sposobów ochrony przed nimi, problematyki związanej z bezpieczeństwem informacji, w tym z codziennym zabezpieczaniem danych i reagowaniem na zagrożenia.

Część 1:

Przygotowanie i przeprowadzenie szkolenia z zakresu świadomości i zagrożeń cyberbezpieczeństwa dla pracowników Urzędu Miejskiego w Będzinie.

1. W ramach realizacji „Części 1” zamówienia Wykonawca zobowiązany będzie do przeprowadzenia stacjonarnego szkolenia z podstaw cyberbezpieczeństwa dla pracowników Urzędu, budującego świadomość cyberzagrożeń i sposobów ochrony.
2. Szkolenia dedykowane są użytkownikom Zamawiającego tj. pracownikom biurowym, pracującym z komputerami i przetwarzającymi różnego rodzaju informacje o różnym poziomie poufności.
3. Celem szkolenia jest budowa świadomości i umiejętności praktycznych pracowników Urzędu w zakresie znajomości różnych rodzajów ataków, sposobów ochrony przed nimi, zasad postępowania w razie ataku oraz problematyki związanej z bezpieczeństwem informacji, w tym z codziennym zabezpieczaniem danych i reagowaniem na zagrożenia.

4. Przeprowadzenie szkoleń ma skutkować zwiększeniem czujności pracowników, lepszą oceną ryzyka oraz umiejętnością postępowania z incydentami w celu zwiększenia świadomości użytkowników i zminimalizowania konsekwencji wynikających z tych ataków. Szkolenie musi obejmować tematykę związaną z cyberbezpieczeństwem, budować świadomość cyberzagrożeń oraz sposobów ochrony przed nimi z uwzględnieniem przyjętych procedur w Urzędzie Miejskim w Będzinie.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. Podstawy cyberbezpieczeństwa:

- podstawowe pojęcia i zasady działania m.in.: phishing, spyware/malware, socjotechnika MFA, spoofing, atak telefoniczny, fałszywe wiadomości mailowe, wyłudzenia BLIK, SMS itp. wraz z przykładami i wskazaniem sposobów przeciwdziałania oraz zabezpieczania się przed powyższymi zagrożeniami,
- opis funkcjonowania zorganizowanych grup cyberprzestępczych,

2. Bezpieczna praca urzędnika:

- metody nieautoryzowanego pozyskania danych wraz z przykładami,
- procesowe podejście do zarządzania w kontekście bezpieczeństwa informacji,
- bezpieczne przetwarzanie danych: szyfrowanie, przechowywanie, udostępnianie, komunikacja,
- stosowanie bezpiecznych haseł, autoryzacja dwuetapowa, klucze sprzętowe,
- rodzaje ataków oraz straty wynikające z udanego ataku,
- groźne ataki 0-day,
- nieopłacona faktura jako sposób przemylenia wirusa do naszego komputera,
- ataki socjotechniczne - czyli niewinne „wyłudzenie” danych,
- przekazywanie haseł dostępowych znajomym,
- cyberbezpieczne korzystanie z poczty,
- bezpieczne korzystanie z urządzeń mobilnych,



- bezpieczna praca zdalna, standardy i najlepsze praktyki postępowania w celu zapewnienia cyberbezpieczeństwa w urzędzie,
- cyberhigiena.

3. Ochrona danych osobowych:

- obowiązki pracownika wynikające z RODO i KRI, ochrona informacji i prywatność w Internecie.

4. Zagrożenia i dezinformacja:

- metody obrony oraz przeciwdziałania (w tym: przed wyludzeniem danych osobowych za pomocą metod socjotechnicznych, oprogramowaniem mogącym zablokować dostęp do urządzeń w urzędzie, szkodliwymi programami mogącymi pozyskać dane osobowe,
- bezpieczeństwo w przeglądarkach, cookies,
- fałszywe wiadomości,
- handel adresami e-mail,
- znaleziony pendrive na parkingu jako pozwolenie na atak dla cyberprzestępcy.

5. Wprowadzenie do SZIB:

- obowiązki pracownika, polityka bezpieczeństwa informacji.

6. Zagrożenia i reakcja:

- identyfikacja zagrożeń, procedury zgłaszania incydentów, przykłady incydentów.

7. Elementy praktyczne:

- studium przypadków, ćwiczenie z rozpoznawania phishingu.

Szkolenie należy przeprowadzić z uwzględnieniem faktu, że uczestnicy szkolenia mogą nie posiadać wiedzy informatycznej i technicznej.

Szkolenie ma obejmować ćwiczenia praktyczne, pozwalające na podniesienie umiejętności związanych z:

- 1) rozpoznawaniem zagrożeń i reagowanie na nie,
- 2) wykorzystywaniem narzędzi informatycznych zapewniających bezpieczeństwo przetwarzanych informacji oraz zabezpieczeń dla poczty elektronicznej i stron WWW,

3) zasadami postępowania w sytuacjach kryzysowych (scenariusze codziennych zagrożeń/ataków).

W trakcie szkolenia trener powinien odpowiadać na pytania uczestników.

Dopuszczalne jest organizowanie sesji pytań i odpowiedzi na zakończenie szkolenia.

W wyniku szkolenia pracownicy mają być w stanie odróżnić typowe błędy techniczne od potencjalnego ataku, wiedzieć jak uniknąć potencjalnego zagrożenia, a w przypadku wystąpienia naruszenia – umieć podjąć podstawowe działania ograniczające skutki wystąpienia incydentu oraz zgłosić incydent do odpowiednich komórek.

Cały materiał szkoleń musi być dostępny w języku polskim i przedstawiony w sposób zrozumiały przez osoby nietechniczne.

Szkolenie musi być na każdym etapie zgodne z zasadami: równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami oraz równości kobiet i mężczyzn.

Każdy uczestnik szkolenia otrzyma od Wykonawcy imienny certyfikat/zaświadczenie z podpisem trenera, potwierdzający ukończenie szkolenia.

Zamawiający wymaga prowadzenia dokumentacji szkolenia.

Na dokumentację szkolenia składają się:

- lista obecności uczestników szkolenia wypełniane oddzielnie dla każdej grupy szkoleniowej,
- lista odbioru certyfikatu/zaświadczenia o ukończeniu szkolenia.

Organizacja szkolenia:

1. Miejsce realizacji szkolenia: Realizując zadanie objęte zamówieniem Wykonawca zobowiązany jest do zapewnienia dostępności architektonicznej poza siedzibą budynku Urzędu Miejskiego w Będzinie, w odległości do 3 km. wraz z zapewnieniem sprzętów elektronicznych m.in.: projektora, rzutnika, dostępu do Internetu.

2. Forma szkoleń: stacjonarna.

3. Liczba osób/uczestników: 82 osoby podzielone na 4 grupy po ok. 20 osób.

5. Czas trwania szkolenia: każda z grup dwa dni, min. 5 h/grupę - jednostką czasową szkolenia jest 1 godzina zegarowa = 60 minut.

6. Termin realizacji: do 4 tygodni od daty zawarcia umowy.

7. Dostęp do platformy szkoleniowej przez min. 6 miesięcy po szkoleniu.

8. Szkolenia muszą odbywać się w dni robocze w godzinach pracy Urzędu w następujących godzinach: poniedziałek 7:30 – 17:00 wtorek – czwartek 7:30-15:30, piątek 7:30 – 14:00.

9. Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika najpóźniej w dniu rozpoczęcia szkolenia. Zamawiający dopuszcza dostarczenie każdemu użytkownikowi kompletu materiałów w formie elektronicznej, np. dokumenty w standardzie PDF. Wszelkie koszty opracowania materiałów szkoleniowych ponosi Wykonawca. Materiały szkoleniowe przekazywane są nieodpłatnie. W celach archiwalnych 1 egzemplarz materiałów zostanie przekazany Zamawiającemu w formie drukowanej oraz udostępni elektronicznie kompletną treść prezentacji multimedialnej wykorzystywanej przez prowadzącego w trakcie szkolenia.

Zamawiający nie ponosi kosztów dojazdu, zakwaterowania oraz wyżywienia Wykonawcy, a także dodatkowych kosztów związanych z przygotowaniem materiałów szkoleniowych.

UWAGI DLA ZADANIA „CZĘŚĆ 1”

- Wykonawca zobowiązany jest przeprowadzić testy sprawdzające wiedzę na wstępie szkolenia i na jego zakończenie. Po zakończeniu szkolenia, zostanie udostępniona ankieta ewaluacyjna szkolenia, a wynik ankiety w formie raportu zostanie przekazany Zamawiającemu.
- 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.

Rezerwacja miejsca prowadzenia zajęć jest po stronie i na koszt Wykonawcy.

- Łączna ilość uczestników szkolenia w części 1 to 82 pracowników wykonujących prace administracyjno – biurowe.
- Wykonawca zobowiązuje się w terminie 7 dni od dnia podpisania umowy dostarczyć Zamawiającemu:

1) szczegółowy zakres merytoryczny szkolenia,

2) 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.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

- Szkolenia będą przeprowadzone po ostatecznej akceptacji dokumentacji przez Zamawiającego.

PO PRZEPROWADZENIU SZKOLENIA DLA DANEJ GRUPY, WYKONAWCA PRZEPROWADZI SYMULACJE PHISINGU KONTROLOWANEGO (na komputerach stacjonarnych pracowników). PO PRZEPROWADZENIU ATAKU PRZEKAŻE WYNIKI W POSTACI NARUSZENIA CYBERBEZPIECZEŃSTWA WRAZ Z DANymi UŻYTKOWNIKA, KTÓRY NIE ZACHOWAŁ OSTROŻNOŚCI I ODCZYTAŁ ZAINFEKOWANĄ WIADOMOŚĆ.

W ramach organizacji szkolenia Wykonawca zapewni:

- 1) autorskie materiały szkoleniowe na zewnętrznych nośnikach pamięci pendrive o pojemności nie mniejszej niż 64 GB oraz pakiet materiałów konferencyjnych, w skład którego wchodzi: fabrycznie nowy długopis oraz notatnik formatu A5 (minimum 20 kartek), umożliwiające swobodne sporządzanie notatek w trakcie szkolenia (materiały zostaną przekazane każdemu uczestnikowi szkolenia nieodpłatnie, na własność).
- 2) serwis kawowy (kawa, herbata, woda, soki, drobne przekąski typu finger food) oraz jeden pełnowartościowy posiłek regeneracyjny (lunch) dla każdego uczestnika w każdym dniu szkoleniowym.
- 3) kadrę trenerską posiadającą wiedzę, doświadczenie i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkolenia,

Realizując niniejsze zamówienie Wykonawca zobowiązany jest do zapewnienia dostępności architektonicznej, cyfrowej oraz informacyjno – komunikacyjnej, osobom ze szczególnymi potrzebami, co najmniej w zakresie określonym przez minimalne wymagania, o których mowa w art. 6 ustawy z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (t.j.Dz. U. z 2024 r. poz. 1411z późn.zm.).

Część 2:

Przygotowanie i przeprowadzenie szkolenia z zakresu SZBI, KRI dla kadry zarządzającej i kierowniczej Urzędu Miejskiego w Będzinie.

1. W ramach realizacji „Części 2” zamówienia Wykonawca zobowiązany będzie do przeprowadzenia stacjonarnego szkolenia z zakresu cyberbezpieczeństwa oraz obowiązków wynikających z wdrożenia Systemu Zarządzania

Bezpieczeństwem Informacji (SZBI) wg norm ISO 27001, 27002, 27005 dla kadry kierowniczej Urzędu Miejskiego w Będzinie.

2. Celem szkolenia jest podniesienie świadomości kadry kierowniczej Urzędu w obszarze cyberbezpieczeństwa poprzez:
 - poznanie różnych rodzajów zagrożeń i typów ataków oraz sposobów ochrony przed nimi,
 - nabycie umiejętności właściwego postępowania w przypadku incydentu bezpieczeństwa,
 - uświadomienie kadrze kierowniczej odpowiedzialności zarządczej w zakresie cyberbezpieczeństwa oraz ochrony danych,
 - przekazanie informacji o nowych technologiach informatycznych wykorzystywanych przez cyberprzestępców,
 - przekazanie aktualnej wiedzy dotyczącej obowiązków wynikających z najnowszych aktów prawnych regulujących bezpieczeństwo informacji i cyberbezpieczeństwo w jednostkach sektora publicznego oraz zasady ich prawidłowej implementacji,
 - budowanie kompetencji w zakresie nadzoru nad wdrażaniem i funkcjonowaniem Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w jednostkach samorządu terytorialnego wg norm ISO 27001, 27002, 27005.

Kadra kierownicza odpowiada za strategiczne decyzje, nadzór oraz operacyjne funkcjonowanie systemów bezpieczeństwa informacji. Specjalistyczne szkolenie ma umożliwić zdobycie wiedzy w zakresie obowiązujących standardów, przepisów prawa oraz dobrych praktyk, w tym zarządzania ryzykiem, reagowania na incydenty oraz zapewnienia ciągłości działania. Bez odpowiedniego przygotowania tej grupy nie jest możliwe skuteczne i trwałe wzmocnienie poziomu cyberbezpieczeństwa jednostki.

W wyniku szkolenia kadra kierownicza musi być w stanie efektywnie zarządzać cyberbezpieczeństwem w urzędzie, podejmować strategiczne decyzje dotyczące ochrony danych oraz promować kulturę bezpieczeństwa wśród pracowników.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. Podstawy cyberbezpieczeństwa oraz przegląd najpopularniejszych zagrożeń:
 - podstawowe pojęcia i zasady działania na temat zagrożeń w sieci takie jak phishing, ransomware, malware, socjotechnika, atak telefoniczny,

spoofing, wyłudzenia BLIK i inne zagrożenia - przykłady i omówienie sposobów przeciwdziałania oraz zabezpieczania się przed powyższymi zagrożeniami,

2. Cyberbezpieczeństwo w ujęciu strategicznym:

- procedury i odpowiedzialność kierownictwa, analiza zagrożeń, kultura bezpieczeństwa, komunikacja z zespołami reagowania,
- organizacja bezpieczeństwa informacji,
- metody wykrywania, reagowania i oceny zagrożeń, kroki do podjęcia w przypadku wykrycia ataku cybernetycznego oraz procedury raportowania incydentów,
- metody obrony oraz przeciwdziałania w tym: przed wyłudzeniem danych osobowych za pomocą metod socjotechnicznych, oprogramowaniem mogącym zablokować dostęp do urządzeń w urzędzie, szkodliwymi programami mogącymi pozyskać dane osobowe,
- ataki socjotechniczne - czyli niewinne „wyłudzenie” danych,

3. Procesy i procedury dotyczące zarządzania incydentami oraz obowiązki poszczególnych osób:

- znaczenie zespołu zarządzającego w obszarze bezpieczeństwa cyfrowego,
- zdarzenia niepożądane, a prawidłowe utrzymanie ciągłości funkcjonowania urzędu,
- zapobieganie atakom cybernetycznym,
- jak chronić swoje urządzenia i systemy (zasoby) przed atakami z zewnątrz,
- alarmy CRP zasady postępowania w razie wprowadzenia stopni dotyczących zagrożeń w cyberprzestrzeni,
- bezpieczne przetwarzanie danych: szyfrowanie, przechowywanie, udostępnianie, komunikacja,
- stosowanie bezpiecznych haseł, autoryzacja dwuetapowa, klucze sprzętowe,
- przewodnik po metodach obrony instytucji,

- opłacalność ataków DoS/DDoS wymierzonych w konkretną instytucję.
4. Prezentacja wymagań Krajowych Ram Interoperacyjności (KRI).
 5. Analiza przepisów rozporządzenia Rady Ministrów z dnia 21 maja 2024 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. 2024 poz. 773) uwzględniając w materiale analizę zmian w stosunku do Rozporządzeniu 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 oraz ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2026 poz. 20) i Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS2).
 - obowiązki jednostek samorządu terytorialnego określone przepisami,
 - cyberbezpieczeństwo jednostki samorządu terytorialnego w kontekście bezpieczeństwa państwa.
 6. Odpowiedzialność prawna kadry kierowniczej:
 - zakres odpowiedzialności administracyjnej, cywilnej, dyscyplinarnej, przykłady konsekwencji naruszeń w jednostkach sektora publicznego.

Organizacja szkolenia:

1. Miejsce realizacji szkolenia: Realizując zadanie objęte zamówieniem Wykonawca zobowiązany jest do zapewnienia dostępności architektonicznej poza siedzibą budynku Urzędu Miejskiego w Będzinie, w odległości do 3 km. wraz z zapewnieniem sprzętów elektronicznych m.in.: projektora, rzutnika, dostępu do internetu.

2. Forma szkoleń: stacjonarna.

3. Liczba osób/uczestników: 30 osób podzielonych na 2 grupy po ok. 15 osób.

5. Czas trwania szkolenia: każda z grup dwa dni, min. 5 h/grupę – jednostką. czasową szkolenia jest 1 godzina zegarowa = 60 minut.

6. Termin realizacji: do 4 tygodni od daty zawarcia umowy.

7. Dostęp do platformy szkoleniowej przez min. 6 miesięcy po szkoleniu.

8. Szkolenia muszą odbywać się w dni robocze w godzinach pracy Urzędu w następujących godzinach: poniedziałek 7:30 – 17:00 wtorek – czwartek 7:30-15:30, piątek 7:30 – 14:00.

UWAGI DLA ZADANIA „CZĘŚĆ 2”

- Zamawiający wymaga prowadzenia dokumentacji szkolenia. Na dokumentację szkolenia składają się: lista obecności uczestników szkolenia oraz lista odbioru certyfikatu/zaświadczenia o ukończeniu szkolenia.
- Zamawiający nie ponosi kosztów dojazdu, zakwaterowania oraz wyżywienia Wykonawcy, a także dodatkowych kosztów związanych z przygotowaniem materiałów szkoleniowych.
- Wykonawca zobowiązany jest przeprowadzić testy sprawdzające wiedzę na wstępie szkolenia i na jego zakończenie. Po zakończeniu szkolenia, zostanie udostępniona ankieta ewaluacyjna szkolenia, a wynik ankiety w formie raportu zostanie przekazany Zamawiającemu.
- 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.

Rezerwacja miejsca prowadzenia zajęć jest po stronie i na koszt Wykonawcy.

- Łączna ilość uczestników szkolenia w części 2 to 30 pracowników - kadra zarządzająca i kierownicza.
- Wykonawca zobowiązuje się w terminie 7 dni od dnia podpisania umowy dostarczyć Zamawiającemu:

1) szczegółowy zakres merytoryczny szkolenia,

2) 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.

PO PRZEPROWADZENIU SZKOLENIA DLA DANEJ GRUPY, WYKONAWCA PRZEPROWADZI SYMULACJE PHISINGU KONTROLOWANEGO (na komputerach stacjonarnych pracowników). PO PRZEPROWADZENIU ATAKU PRZEKAŻE WYNIKI W POSTACI NARUSZENIA CYBERBEZPIECZEŃSTWA WRAZ Z DANymi UŻYTKOWNIKA, KTÓRY NIE ZACHOWAŁ OSTROŻNOŚCI I ODCZYTAŁ ZAINFEKOWANĄ WIADOMOŚĆ.

W ramach organizacji szkolenia Wykonawca zapewni:

- 1) autorskie materiały szkoleniowe na zewnętrznych nośnikach pamięci pendrive o pojemności nie mniejszej niż 64 GB oraz pakiet materiałów konferencyjnych, w skład którego wchodzi: fabrycznie nowy długopis oraz notatnik formatu A5 (minimum 20 kartek), umożliwiające swobodne sporządzanie notatek w trakcie szkolenia (materiały zostaną przekazane każdemu uczestnikowi szkolenia nieodpłatnie, na własność).
- 2) serwis kawowy (kawa, herbata, woda, soki, drobne przekąski typu finger food) oraz jeden pełnowartościowy posiłek regeneracyjny (lunch) dla każdego uczestnika w każdym dniu szkoleniowym.
- 3) dostęp do platformy szkoleniowej przez min. **6 miesięcy po szkoleniu**.
- 4) wydanie Zamawiającemu zaświadczeń/certyfikatu o ukończeniu szkolenia dla każdego uczestnika,
- 5) kadrę trenerską posiadającą wiedzę, doświadczenie i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkolenia,

Realizując niniejsze zamówienie Wykonawca zobowiązany jest do zapewnienia dostępności architektonicznej, cyfrowej oraz informacyjno – komunikacyjnej, osobom ze szczególnymi potrzebami, co najmniej w zakresie określonym przez minimalne wymagania, o których mowa w art. 6 ustawy z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (t.j. Dz. U. z 2024 r. poz. 1411 z późn. zm.).

Część 3.

Przygotowanie i przeprowadzenie szkolenia z zakresu etycznego hackingu i cyberbezpieczeństwa (poziom zaawansowany) dla zespołu IT Urzędu Miejskiego w Będzinie.

- Przedmiotem zamówienia jest realizacja specjalistycznego szkolenia z zakresu **etycznego hackingu (ethical hacking) oraz testów penetracyjnych**, ukierunkowanego na rozwój kompetencji w obszarze **cyberbezpieczeństwa systemów informatycznych**, wraz z przygotowaniem uczestników do uzyskania **międzynarodowego certyfikatu branżowego**.
- Szkolenie powinno obejmować zarówno komponent teoretyczny, jak i **intensywną część praktyczną realizowaną w środowisku laboratoryjnym (hands-on labs)**.

Celem szkolenia jest:

- nabycie zaawansowanej wiedzy w zakresie identyfikacji i analizy zagrożeń cybernetycznych,
- rozwój umiejętności wykrywania podatności oraz przeprowadzania testów penetracyjnych, poznanie metod działania cyberprzestępców w celu skuteczniejszej ochrony systemów,
- wykorzystanie narzędzi wspieranych sztuczną inteligencją (AI) w cyberbezpieczeństwie,
- przygotowanie uczestników do zdania egzaminu certyfikacyjnego.

Szkolenie musi obejmować co najmniej następującą tematykę:

Moduły obowiązkowe (minimum 20 obszarów tematycznych):

1. Wprowadzenie do etycznego hackingu
2. Rekonesans i pozyskiwanie informacji (Footprinting & Reconnaissance)
3. Skanowanie sieci
4. Enumeracja zasobów
5. Analiza podatności (Vulnerability Analysis)
6. Ataki na systemy operacyjne (System Hacking)
7. Zagrożenia malware
8. Sniffing i analiza ruchu sieciowego
9. Socjotechnika (Social Engineering)
10. Ataki typu DoS/DDoS
11. Przejmowanie sesji (Session Hijacking)

12. Omijanie systemów zabezpieczeń (IDS, firewall, honeypoty)
13. Bezpieczeństwo serwerów webowych
14. Bezpieczeństwo aplikacji webowych
15. Ataki SQL Injection
16. Bezpieczeństwo sieci bezprzewodowych
17. Bezpieczeństwo urządzeń mobilnych
18. Bezpieczeństwo IoT i OT
19. Bezpieczeństwo chmury
20. Podstawy kryptografii

Organizacja szkolenia:

1. **Forma szkoleń:** stacjonarna
2. **Liczba osób/uczestników:** 3 osoby
3. **Czas trwania szkolenia:** minimum 5 dni szkoleniowych (min. 40 godzin dydaktycznych – jednostką czasową szkolenia jest 1 godzina zegarowa = 60 minut)
4. **Termin realizacji:** do 4 tygodni od daty zawarcia umowy.
5. **Szkolenie musi obejmować:**
 - dostęp do **wirtualnych laboratoriów (labs)**,
 - ćwiczenia praktyczne oparte na rzeczywistych scenariuszach,
 - pracę na narzędziach wykorzystywanych w testach penetracyjnych,
 - dostęp do platformy szkoleniowej przez min. **6 miesięcy po szkoleniu**.
6. Szkolenia muszą odbywać się w dni robocze w godzinach pracy Urzędu w następujących godzinach: poniedziałek 7:30 – 17:00 wtorek – czwartek 7:30-15:30, piątek 7:30 – 14:00.
7. **Organizator zapewni:** serwis kawowy (kawa, herbata, woda, soki, drobne przekąski typu finger food) oraz jeden pełnowartościowy posiłek regeneracyjny (lunch) dla każdego uczestnika, w każdym dniu szkoleniowym.

Wymagania dotyczące materiałów i narzędzi:

Wykonawca zapewni:

- komplet materiałów szkoleniowych (elektronicznych lub drukowanych),
- dostęp do środowiska laboratoryjnego,
- dostęp do narzędzi symulujących rzeczywiste środowiska cyberzagrożeń,
- możliwość realizacji ćwiczeń praktycznych i case studies.

Certyfikacja i egzamin:

W ramach zamówienia Wykonawca zapewni:

- voucher na egzamin certyfikacyjny (ważny min. 12 miesięcy),
- przygotowanie do egzaminu teoretycznego (MCQ),
- możliwość przystąpienia do egzaminu praktycznego (w wersji rozszerzonej),
- dostęp do platform egzaminacyjnych (np. Pearson VUE lub równoważnych).

Wymagania wobec Wykonawcy:

Wykonawca musi:

- posiadać doświadczenie w realizacji szkoleń z zakresu cyberbezpieczeństwa,
- realizować szkolenia zgodne z uznanymi standardami międzynarodowymi,
- dysponować trenerami: z certyfikatami z zakresu cyberbezpieczeństwa (np. CEH lub równoważne),
- posiadającymi min. 2–3 lata doświadczenia praktycznego,
- zapewnić program szkolenia zgodny z aktualnymi trendami cyberzagrożeń.

Efekty szkolenia:

Po zakończeniu szkolenia uczestnik:

- potrafi identyfikować podatności systemów IT,
- zna metody przeprowadzania testów penetracyjnych,
- rozumie mechanizmy cyberataków,

- potrafi wykorzystać narzędzia bezpieczeństwa i AI,
- jest przygotowany do uzyskania certyfikatu branżowego.

Kryteria równoważności

Zamawiający dopuszcza rozwiązania równoważne pod warunkiem, że:

- program szkolenia obejmuje co najmniej wskazany zakres tematyczny,
- szkolenie kończy się możliwością uzyskania certyfikatu rozpoznawalnego międzynarodowo,
- zapewnione są laboratoria praktyczne i środowisko symulacyjne,
- poziom szkolenia odpowiada poziomowi zaawansowanemu.

Dodatkowe wymagania (opcjonalne – punktowane w ocenie ofert)

- dostęp do platform typu CTF (Capture The Flag),
- możliwość udziału w wyzwaniach cyberbezpieczeństwa,
- rozszerzony pakiet szkoleniowy (np. dodatkowe materiały wideo),
- możliwość jednego bezpłatnego powtórzenia egzaminu.

UWAGI DLA ZADANIA „CZĘŚĆ 3”

- Zamawiający wymaga prowadzenia dokumentacji szkolenia. Na dokumentację szkolenia składają się: lista obecności uczestników szkolenia oraz lista odbioru certyfikatu/zaświadczenia o ukończeniu szkolenia.
- Zamawiający nie ponosi kosztów dojazdu, zakwaterowania oraz wyżywienia Wykonawcy, a także dodatkowych kosztów związanych z przygotowaniem materiałów szkoleniowych.
- 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.

Rezerwacja miejsca prowadzenia zajęć jest po stronie i na koszt Wykonawcy.

- Łączna ilość uczestników szkolenia w części 3 to 3 pracowników IT.

- Wykonawca zobowiązuje się w terminie 7 dni od dnia podpisania umowy dostarczyć Zamawiającemu:

1) szczegółowy zakres merytoryczny szkolenia,

2) 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.

Będzin, dnia 23 kwietnia 2026 r.

Z up. PREZYDENTA MIASTA BĘDZINA
WICEPREZYDENT MIASTA

Aneta
Aneta Złocka

ZASTĘPCA NACZELNIKA
Wydziału Organizacyjnego

Beata Świątek
Beata Świątek

SEKRETARZ MIASTA

Magdalena Rogawicz
Magdalena Rogawicz