



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Załącznik nr 3
do Zapytania ofertowego
SAO.042.1.4.2026

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest przeprowadzenie szkoleń w formule on-line z zakresu cyberbezpieczeństwa dla pracowników Urzędu Miasta i podległych mu następujących 13 jednostek organizacyjnych Gminy Miejskiej Hajnówka:
 - a) Szkoła Podstawowa Nr 1 im. Janusza Kusocińskiego, ul. 3 Maja 54, 17-200 Hajnówka,
 - b) Szkoła Podstawowa Nr 2 im. Władysława Jagiełły w Hajnówce, ul. W. Wróblewskiego 2, 17-200 Hajnówka.
 - c) Szkoła Podstawowa Nr 3 im. dr. Kazimierza Ptaszyńskiego w Hajnówce, ul. Działowa 1,
 - d) Szkoła Podstawowa Nr 4 im. Henryka Sienkiewicza w Hajnówce, ul. Nowowarszawska 20, 17-200 Hajnówka,
 - e) Przedszkole Nr 1 w Hajnówce, ul. Władysława Jagiełły 7, 17-200 Hajnówka,
 - f) Przedszkole Nr 2 im. Kubusia Puchatka w Hajnówce, ul. Warszawska 2, 17-200 Hajnówka,
 - g) Przedszkole Nr 3 im. Żubra Pompika z Oddziałami Integracyjnymi w Hajnówce, ul. Reczna 3, 17-200 Hajnówka,
 - h) Przedszkole N4 5 w Hajnówce, ul. M. Reja 2, 17-200 Hajnówka,
 - i) Żłobek Samorządowy w Hajnówce, ul. Armii Krajowej 24, 17-200 Hajnówka,
 - j) Park Wodny w Hajnówce, ul. 3 Maja 50, 17-200 Hajnówka,
 - k) Ośrodek Sportu i Rekreacji w Hajnówce, ul. Ks. A. Dziewiatowskiego 2, 17-200 w Hajnówce,
 - l) Zakład Gospodarki Mieszkaniowej, ul. Parkowa 6, 17-200 Hajnówka,
 - m) Miejski Ośrodek Pomocy Społecznej w Hajnówce, ul. 11 Listopada 24, 17-200 Hajnówka,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”) - Zadanie 2 - Działania podnoszące kompetencje JST w zakresie cyberbezpieczeństwa.
2. Zamawiający wymaga przeprowadzenia dwóch rodzajów szkoleń:
 - 1) dla wszystkich pracowników Zamawiającego (ok. 450 osób, w tym ok. 350 osób pracujących przy komputerach i 100 osób pracujących bez komputerów) – szkolenia z zakresu podstawowego, dostosowane do wiedzy i świadomości przeciętnie rozeznanej osoby;



- 2) dla kadry kierowniczej Zamawiającego – kierownicy i dyrektorzy, pracownicy IT (ok. 40 osób) – szkolenie z zakresu zaawansowanego, dostosowane do wiedzy specjalistycznej odbiorców szkolenia oraz dostosowane do zagrożeń, z którymi ta kategoria pracowników może się zetknąć wykonując swoją pracę.
3. Szkolenia powinny składać się z części teoretycznej.
4. Szkolenia odbędą się w formule online.
5. Szkolenia muszą być dedykowane dla jednostek samorządu terytorialnego, w tym jednostkom wymienionym w pkt. 1 a) – m) niniejszego opisu przedmiotu zamówienia i przeprowadzone przez doświadczonych trenerów posiadających stosowną wiedzę oraz co najmniej 2-letnie doświadczenie w przeprowadzaniu szkoleń z zakresu cyberbezpieczeństwa oraz posiadających uprawnienia wymagane przez Projekt.
6. Zleceniodawca nie zgadza się na zlecenie przedmiotu umowy podmiotowi trzeciemu.
7. Szkolenia muszą odbyć się w terminie do dnia 23 września 2026 r., w dni robocze od poniedziałku do piątku, w godzinach zbliżonych do 8:00 – 15:00. Dokładny termin zostanie uzgodniony z Wykonawcą po podpisaniu umowy.
8. Szkolenia muszą odbywać się w grupach do 50 osób.
9. Wykonawca jest zobowiązany do obsługi procesu rejestracji online za pośrednictwem dedykowanego systemu lub drogą mailową oraz do bieżącej kontroli limitu miejsc, który wynosi maksymalnie 50 osób w pojedynczej grupie szkoleniowej. Wykonawca musi zapewnić, aby formularz rejestracyjny lub lista uczestników zawierały informację określającą jednostkę miejską, z której pochodzi dana osoba.
10. Każde ze szkoleń powinno trwać 6 godzin zegarowych, wliczając w to 1 godzinę na przerwy.
11. Ilekroć w niniejszym opisie przedmiotu zamówienia mowa jest o „Wykonawcy”, należy przez to rozumieć również „Dostawcę szkolenia”, tj. zarówno podmiot świadczący usługi szkoleniowe, jak i osobę bezpośrednio realizującą szkolenie, dalej łącznie zwanych „Wykonawcą”.
- 12. Szkolenie dla pracowników Urzędu Miasta Hajnówka i jednostek podległych Zamawiającego (zakres podstawowy) obejmuje informacje z zakresu:**
 - a) Bezpieczeństwa informacji – podstawowe wiadomości, z uwzględnieniem regulacji wewnętrznych oraz wymagań rozporządzenia KRI,
 - b) Wewnętrznych procedur w obszarze bezpieczeństwa informacji cyberbezpieczeństwa,
 - c) Wymagań dla pracowników wynikające z KRI, uoKSC oraz RODO,
 - d) Systemu Zarządzania Bezpieczeństwem Informacji w praktyce,
 - e) Przeglądu najpopularniejszych zagrożeń i zasady bezpiecznego korzystania z internetu,
 - f) Ochrony informacji i prywatności w internecie,
 - g) Ransomware jako poważne zagrożenie dla JST,
 - h) Phishingu, oszustw i wyłudzeń z uwzględnieniem oszustwa typu BEC (Business E-mail Compromise),
 - i) Cyberhigieny, w tym bezpieczeństwo urządzeń i bezpieczeństwo fizyczne,
 - j) Bezpiecznych haseł i uwierzytelnienia dwuskładnikowego,
 - k) Wewnętrznych zaleceń i rekomendacji, w tym sposobów reakcji na incydenty bezpieczeństwa.



13. Szkolenie dla kadry zarządzającej i pracowników IT Zamawiającego (zakres zaawansowany) obejmuje informacje z zakresu:

- a) Podstaw prawnych cyberbezpieczeństwa,
- b) Wymogów wynikających z KRI, uoKSC i RODO,
- c) Przeglądu znanych typów ataków na JST,
- d) Przeglądu nowoczesnych narzędzi i usług cyberbezpieczeństwa (jako wsparcie procesu zakupowego),
- e) Zarządzaniu ryzykiem w bezpieczeństwie informacji i obszarach technicznych,
- f) Systemie Zarządzania Bezpieczeństwem Informacji – jak skutecznie wdrożyć SZBI,
- g) Ciągłości działania – dlaczego jest istotna i jak ją wdrożyć,
- h) Współpracy w ramach s46,
- i) Identyfikowania zagrożeń – jak wdrożyć odpowiednie zabezpieczenia,

14. Szczegółowy zakres szkolenia teoretycznego dla pracowników IT powinien obejmować co najmniej następujące zagadnienia:

- a) Podstawy bezpieczeństwa sieci,
- b) Aspekty techniczne najpopularniejszych ataków i metody reagowania,
- c) Zabezpieczanie poczty elektronicznej,
- d) Zabezpieczanie serwisów www,
- e) Ochrona przed atakami DdoS,
- f) Profilaktyka cyberzagrożeń ze szczególnym uwzględnieniem zarządzania kopiami zapasowymi,
- g) Przegląd źródeł wiedzy o zagrożeniach,
- h) Podstawy zabezpieczenia ciągłości działania,
- i) Identyfikacja podatności i aktualizacja oprogramowania,
- j) Zarządzanie incydemem.

- 15. Kadra kierownicza i pracownicy IT mogą stanowić jedną grupę szkoleniową.
- 16. Po zakończeniu szkolenia, zostanie udostępniona ankieta ewaluacyjna szkolenia, a wynik ankiety w formie raportu zostanie przekazany Zamawiającemu.
- 17. Wykonawca po zakończeniu szkoleń prześle Zleceniodawcy w formie elektronicznej: certyfikaty ukończenia szkoleń osobom, które wzięły udział w szkoleniu, listy obecności, program szkolenia, prezentację i ewentualne materiały szkoleniowe.
- 18. Przed rozpoczęciem szkoleń każdy z jego uczestników musi mieć możliwość pobrania materiałów szkoleniowych.
- 19. Wszelkie dokumenty dotyczące zapytania ofertowego muszą być oznaczone logotypami przesłanymi Wykonawcy przez Zamawiającego.
- 20. Wykonawca jest zobowiązany w terminie do 3 dni roboczych po zakończeniu realizacji Przedmiotu zamówienia dostarczyć Zamawiającemu dokumenty wskazane w pkt. 14 i 15 .
- 21. Wykonawca zobowiązuje się w terminie 7 dni od dnia podpisania umowy dostarczyć Zamawiającemu:
 - 1) proponowane terminy szkolenia;



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

- 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.

22. Wykonawca zobowiązany jest do zapewnienia i pokrycia pełnych kosztów wszelkich zasobów niezbędnych do prawidłowej oraz terminowej realizacji zamówienia. W cenie oferty Wykonawca musi uwzględnić w szczególności: koszty wynagrodzenia trenera/prowadzącego szkolenie, koszty udostępnienia i obsługi interaktywnej platformy szkoleniowej online (wraz z niezbędnymi licencjami i dostępami dla uczestników), koszty przygotowania i udostępnienia materiałów szkoleniowych w formie elektronicznej, a także wszelkie inne koszty techniczne, organizacyjne i administracyjne niezbędne do przeprowadzenia szkolenia w formule zdalnej. Zamawiający nie ponosi żadnych dodatkowych kosztów z tytułu przygotowania i przeprowadzenia przedmiotowych szkoleń.