Miasto Malbork,
z siedzibą Urzędu Miasta Malbork
przy Plac Słowiańskim 5,
82-200 Malbork,
woj. pomorskie, Polska,
NIP: 579-22-30-763,
Regon 170747827

Zapytanie ofertowe

nr 1/WPR/2024 na:

przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa
dla kadry kierowniczej i pracowników Urzędu Miasta Malbork oraz jednostek podległych.

o wartości nie przekraczającej wyrażonej w złotych równowartości kwoty określonej
w art. 2 ust. 1 pkt 1) ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych
(tekst jednolity 2024 poz.1320)
Opublikowane na stronie Bazy konkurencyjności
https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Malbork, 15.10. 2024 r.

1. Nazwa i dane adresowe Zamawiającego

Zamawiający:	Miasto Malbork
Adres:	Przy Plac Słowiański 5 82-200 Malbork
Telefon:	+48 55 6290400
E-mail:	magistrat@um.malbork.pl
ESP (ePUAP)	/ /ESP Adres skrytki ePUAP: /xt2uer311q/SkrytkaESP
Strona internetowa:	www.urzad.malbork.pl
Strona BIP:	www.bip.malbork.pl
NIP:	579-22-30-763
REGON:	170747827

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

2. Wstęp

Zamówienie jest realizowane w ramach grantu w projekcie grantowym **„Cyberbezpieczny Samorząd”** współfinansowanym przez Unię Europejską z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: *Zaawansowane usługi cyfrowe*, Działanie 2.2. – *Wzmocnienie krajowego systemu cyberbezpieczeństwa*, na podstawie umowy o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/1512 W ramach projektu przewidziano kompleksowe przeszkolenie i zakup platformy szkoleniowej z zakresu cyberbezpieczeństwa w celu zapewnienia regularnego podnoszenia poziomu świadomości cyberbezpieczeństwa u pracowników Urzędu Miejskiego w Malborku oraz jednostek podległych:

- Miejski Ośrodek Pomocy Społecznej u. Słowackiego 74, 82-200 Malbork
- Centrum Usług Wspólnych przy Plac Słowiański 5, 82-200 Malbork
- SP 1 Malbork, Żeromskiego 45 82-200 Malbork
- SP 2 Aleja Wojska Polskiego 479, 82-200 Malbork
-SP 3 Stanisława Hadyny 18, 82-200 Malbork
-SP 6 Tczewska 13, 82-200 Malbork
-SP 8 Generała de Gaulle'a 91, 82-200 Malbork
-SP 9 Plac Gabriela Narutowicza 15, 82-210 Malbork
-Ośrodek Sportu i Rekreacji Toruńska 60, 82-200 Malbork

3. TRYB UDZIELENIA ZAMÓWIENIA:

1. Na podstawie art. 2 ust. 1 pkt. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych niniejsze postępowanie nie podlega przepisom ww. ustawy.
2. Postępowanie przeprowadzone jest na stronie Bazy Konkurencyjności w progach 50 000

zł netto – 130 000 zł https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl

3. Oznaczenie wg Wspólnego Słownika Zamówień (kod CPV):
   80510000-2 Usługi szkolenia specjalistycznego

   79632000-3 Szkolenie pracowników

4. Zamawiający dopuszcza składanie ofert częściowych. Liczba części: 2. Dopuszcza się składanie ofert przez wykonawcę na wszystkie części zamówienia.

5. Zamawiający nie dopuszcza składania ofert wariantowych.

   Zamawiający przewiduje udzielanie zamówień podobnych w wysokości 100% zamówienia podstawowego.

6. Postępowanie prowadzone jest w języku polskim, w portalu Baza Konkurencyjności: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl

4. Wymagania ogólne (do wszystkich części zamówienia)

We wszystkich częściach zamówienia muszą zostać zachowane zasady równości szans i niedyskryminacji, w tym dostępność dla osób z niepełnosprawnościami oraz równości kobiet i mężczyzn. W przypadku szkoleń online, e-learningu (dostęp do platformy szkoleniowej) wymagane będzie spełnienie przez wykonawcę wymogów dostępności oraz WCAG 2.1 dla narzędzi/platform które zostaną wykorzystane do szkoleń. W sytuacji kiedy szkolenia będą prowadzone w formie stacjonarnej wykonawca będzie musiał zapewnić materiał szkoleniowy z większym rozmiarem czcionki (w zależności od potrzeb uczestników szkolenia). Opracowane dokumentacje będą musiały być dostarczone w elektronicznej z możliwością powiększania treści.

Wykonawca każdej z części zamówienia będzie zobowiązany do podpisania oświadczenia potwierdzającego przestrzeganie powyższych zasad.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

5. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest przeprowadzenie stacjonarnych szkoleń z zakresu cyberbezpieczeństwa dla kadry kierowniczej i pracowników IT Urzędu, zakupu platformy szkoleniowej dla pracowników Urzędu Miasta Malborka oraz jednostek podległych. Zamówienie obejmuje zakup dostępu do platformy szkoleniowej, na której pracownicy będą mogli na bieżąco szkolić się z zakresu cyberbezpieczeństwa.

Przedmiot zamówienia jest podzielony na 2 części. Ocena ofert zostanie przeprowadzona dla każdej części z osobna. Wykonawcy mogą składać oferty na dowolną liczbę części.

Szkolenia (części 1. – 2. zamówienia) muszą spełniać następujące wymagania:

1. Miejscem realizacji dla części 1 zamówienia jest siedziba Urzędu Miejskiego w Malborku przy ul. Plac Słowiański 5, 82-200 Malbork. Zamawiający może dopuścić zmianę miejsca realizacji szkolenia lub jego formy w przypadku sytuacji nadzwyczajnych (pandemia, klęska żywiołowa, wprowadzenie stanu wyjątkowego, wojny, itp.), uniemożliwiających przeprowadzenie szkolenia stacjonarnego w Urzędzie. Miejscem realizacji dla części 2 – zakup szkolenia dziedzinowego dla pracownika IT jest siedziba zamawiającego bądź możliwość szkolenia zdalnego na wniosek zamawiającego.
2. Szkolenia dla części 1 muszą odbywać się w godzinach pracy Urzędu.
3. Wykonawca w ramach wykonania usługi przedstawi szczegółowy program szkolenia zawierający informacje dotyczące tematyki i czasu szkolenia, i dostarczy go w terminie nie później niż 7 dni roboczych przed dniem rozpoczęcia szkolenia do akceptacji Zamawiającego.
4. Opracowane materiały będą musiały być dostarczone w formie elektronicznej z możliwością powiększania treści. W ramach wynagrodzenia Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika, pozwalające na samodzielną edukację z zakresu tematyki szkolenia. Zamawiający dopuszcza dostarczenie kompletu materiałów w formie elektronicznej, np. dokumenty w standardzie PDF.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

5. Wykonawca dostarczy materiały szkoleniowe uczestnikom szkolenia najpóźniej w dniu rozpoczęcia szkolenia.
6. W ramach wynagrodzenia Wykonawca dostarczy Zamawiającemu materiały ze szkolenia, które to będzie mógł wykorzystać do przeszkolenia osób nieobecnych lub nowoprzyjętych.
7. Wykonawca nie jest zobowiązany do zapewnienia uczestnikom wyżywienia podczas szkoleń stacjonarnych.
8. Każdy uczestnik szkolenia otrzyma od Wykonawcy imienny certyfikat, potwierdzający ukończenie szkolenia i jego zakres.
9. Zamawiający zwraca uwagę, że szkolenia będące przedmiotem zamówienia mają charakter kształcenia zawodowego i są finansowane w minimum 70% ze środków publicznych, w związku z czym są one zwolnione z podatku od towarów i usług na podstawie §3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 roku w sprawie zwolnień od podatku towarów i usług oraz warunków stosowania tych zwolnień (t.j. Dz.U. 2023 poz. 955).

5.1. Część 1.: Szkolenia dla kadry kierowniczej Urzędu i pracowników IT

W ramach realizacji części 1. zamówienia Wykonawca zobowiązany będzie do przeprowadzenia **szkolenia specjalistycznego** dla kadry kierowniczej oraz pracowników IT w zakresie bezpieczeństwa informacji i wymogów w zakresie cyberbezpieczeństwa. Celem szkolenia jest zwiększenie świadomości kadry kierowniczej Urzędu w zakresie problematyki związanej z bezpieczeństwem informacji, rozwinięcie umiejętności strategicznego zarządzania cyberbezpieczeństwem oraz zrozumienie przepisów prawnych i ich implementacji.

Szkolenie powinno być kompleksowym procesem, który umożliwia uczestnikom zdobycie dogłębnej wiedzy na temat wybranych zagadnień. Powinno ono nie tylko dostarczyć podstawowej informacji, ale także omówić zaawansowane aspekty danej tematyki, aby uczestnicy mieli pełniejsze zrozumienie tematu i byli w stanie zastosować zdobytą wiedzę w praktyce. Przekazywanie wiedzy powinno być interaktywne i angażujące, wykorzystując różnorodne metody nauczania, takie jak prezentacje, dyskusje, studia przypadków czy praktyczne ćwiczenia, co

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

pozwoli uczestnikom efektywniej przyswoić omawiany materiał.

W ramach przeprowadzonego szkolenia wykonawca powinien zaprezentować:

1. Podstawowe informacje o obecnej sytuacji rynkowej powiązanej z tematyką cyberbezpieczeństwa:

- Podstawy i definicje: zapewnienie uczestnikom solidnych podstaw w dziedzinie cyberbezpieczeństwa poprzez omówienie kluczowych pojęć i zasad. Ponadto, zostanie przedstawiona rola menedżera w formowaniu bezpiecznego środowiska cyfrowego, co pozwoli zrozumieć jak ważne jest aktywne zaangażowanie kierownictwa w procesy zapewnienia bezpieczeństwa informacji. W ten sposób uczestnicy będą mieć pełniejsze zrozumienie zarówno teoretycznych, jak i praktycznych aspektów cyberbezpieczeństwa oraz będą lepiej przygotowani do podejmowania decyzji w tym obszarze.

- Statystyki i trendy: skoncentrowanie się na przekazaniu uczestnikom szczegółowej analizy globalnych i lokalnych danych dotyczących cyberataków. Poprzez omówienie ewolucji tych ataków oraz ich metodologii, uczestnicy zyskają wgląd w aktualne trendy i sposoby działania cyberprzestępców. Ponadto, zostaną przedstawione skutki, jakie cyberatak może mieć dla biznesu, co pozwoli uczestnikom lepiej zrozumieć znaczenie inwestycji w bezpieczeństwo informacji oraz skuteczne zarządzanie ryzykiem cybernetycznym dla organizacji. Dzięki temu będą mogli podejmować bardziej świadome decyzje w zakresie ochrony swoich danych i infrastruktury cyfrowej.

2. Omówienie światowych standardów i norm w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji.

- Normy ISO/IEC: Szczegółowe omówienie serii norm: ISO/IEC 27000: (zarysowuje leksykon oraz globalne zasady nadrzędne systemu zarządzania bezpieczeństwem informacji, kreśląc fundament pod szersze zrozumienie oraz efektywniejsze stosowanie pozostałych norm z rodziny 27000), ISO/IEC 27001 (stanowi kanon dotyczący wymagań dla systemów zarządzania bezpieczeństwem informacji, umożliwiając organizacjom zabezpieczenie informacji pod kątem ich poufności, integralności oraz dostępności przez implementację adekwatnych procedur zarządczych), ISO/IEC 27002 (oferuje referencyjny zbiór praktyk dla organizacji dążących do identyfikacji, wdrażania, utrzymania oraz doskonalenia swoich mechanizmów ochrony informacji w kontekście SZBI), ISO/IEC 27004 (dostarcza metodykę do monitorowania, przeglądu, oceny oraz doskonalenia efektywności systemu zarządzania bezpieczeństwem informacji, akcentując znaczenie mierzalnych wskaźników), ISO/IEC 27005 (zawiera wytyczne dotyczące zarządzania

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

ryzykiem w kontekście bezpieczeństwa informacji, nakreślając proces identyfikacji, oceny oraz zarządzania ryzykiem informacyjnym), ISO/IEC 27006 (określa wymogi dla organizacji świadczących usługi certyfikacji systemów zarządzania bezpieczeństwem informacji, wyznaczając ramy dla procesu audytu i certyfikacji), ISO/IEC 27013 (podaje wytyczne integrujące system zarządzania bezpieczeństwem informacji z systemem zarządzania usługami IT, promując koherentną i efektywną infrastrukturę zarządzania), ISO/IEC 27017 (koncentruje się na bezpieczeństwie informacji w chmurze, proponując kontrole oraz wytyczne dla dostawców i użytkowników usług przetwarzania w chmurze), ISO/IEC 27018 (ustanawia kodeks praktyk dla ochrony informacji osobowych w chmurze, zgodnie z wymaganiami prywatności i ochrony danych), ISO/IEC 22301 (specyfikuje wymogi dla systemów zarządzania ciągłością działania, umożliwiając organizacjom przygotowanie na incydenty zakłócające normalne funkcjonowanie), ISO/IEC 24762 (zawiera wytyczne dla usług odzyskiwania po awariach w centrach danych i innych środowiskach IT, podkreślając kluczowe elementy potrzebne do przywrócenia operacji IT po katastrofie, ISO/IEC 27036 (skupia się na zarządzaniu bezpieczeństwem informacji w relacjach między organizacjami, oferując wytyczne dotyczące bezpieczeństwa w outsourcingu i partnerstwach biznesowych), ISO/IEC 31000 (dostarcza wytyczne dotyczące zarządzania ryzykiem ogólnym, promując model zarządzania ryzykiem, który można dostosować do różnych typów organizacji i kontekstów), 13501-2 (norma ta przeprowadza proces kategoryzacji reakcji na ogień wyrobów używanych w budownictwie oraz elementów konstrukcyjnych budowli, określając ich parametry odporności na pożary i zachowanie w ekstremalnych warunkach termicznych), norma 1627 (stanowi kryteria odporne na nieautoryzowany dostęp przez systemy zamykające, jak okna, drzwi oraz osłony, hierarchizując je zgodnie z ich zdolnością do stawiania oporu przy próbach sforsowania), norma 12209-04 (wytycza wymagania techniczne oraz procedury badawcze dla mechanizmów blokujących w obszarze budowlanym, takich jak zamki mechaniczne wraz z ich komponentami, oceniając ich funkcjonalność oraz niezawodność.), norma 50131-1 (określa specyfikacje dla systemów alarmowych przeznaczonych do sygnalizacji prób włamania czy napadu, wyznaczając standardy dotyczące ich skuteczności oraz metodyki testowania).

- Omówienie znaczenia powyższych norm i ich w zapewnianiu wysokiego poziomu bezpieczeństwa informacji oraz praktycznego zastosowania w organizacjach.

- Inne standardy: Przedstawienie i dyskusja na temat innych standardów:

- ramy dotyczące zarządzania ryzykiem cyberbezpieczeństwa - NIST Cybersecurity Framework;

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

- ramy dotyczące wdrażania, rozwoju i doskonalenia polityki IT – COBIT;
- zbiór praktyk dotyczący zarządzania usługami IT – ITIL;
- akceptowalna polityka szyfrowania SANS;
- techniki kryptograficzne - ENISA ;
- ramy ochrony informacji i zasobów federalnych agencji rządowych USA - 800-53 rev3.

- Rola powyższych zagranicznych standardów w kształtowaniu efektywnych polityk bezpieczeństwa w organizacjach.

3. Omówienie zaawansowanych strategii ochrony organizacji:

- Zarządzanie ryzykiem: Metody identyfikacji, oceny, mitygacji i monitorowania ryzyka cybernetycznego. Wykorzystanie narzędzi i technologii do analizy ryzyka.

- Szczegółowy opis i kroki zarządzania incydentami:

- wykrywanie: inicjacja procesu inicjującego, mającego na celu detekcję niestandardowych aktywności lub zdarzeń infrastrukturalnych, które mogą sygnalizować potencjalne zagrożenia w obszarze cybernetycznym;
- rejestrowanie: operacja dokumentacyjna, polegająca na chronologicznym zapisie zaobserwowanych dysfunkcji w dedykowanych bazach danych, by zapewnić dokumentację dowodową dla późniejszych faz postępowania;
- analizowanie: metodyczne badanie zgromadzonych artefaktów zdarzeń w celu zrozumienia ich genezy, dynamiki oraz wpływu na ekosystem informacyjny;
- klasyfikowanie: systematyzacja incydentów według ustalonego kodu klasyfikacyjnego, uwzględniająca ich naturę, zasięg oraz potencjalne konsekwencje dla organizacji.
- priorytetyzowanie: alokacja zasobów reakcyjnych na bazie oceny krytyczności, która koresponduje z możliwymi konsekwencjami incydentu dla misji instytucji;
- podejmowanie działań naprawczych: inicjowanie interwencji korygujących mających na celu restytucję funkcji systemowych i prewencję przed podobnymi naruszeniami w przyszłości;
- ograniczanie skutków incydentu: implementacja taktyk zaradczych, które mają za zadanie minimalizację negatywnych rezultatów incydentu oraz odbudowę stanu równowagi operacyjnej.

- Priorytetyzacja incydentów na 3 kategorie: krytyczny, wysoki, średni na podstawie poniższych opisów:

- **Priorytet krytyczny** - Incydent wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT. Procesy wewnętrzne są sparaliżowane lub zakłócone w znaczącym

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

stopniu. Istnieje wysokie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.

- **Priorytet wysoki** - Incydent wymaga szybkiego działania oraz zgłoszenia do właściwego CSIRT w ciągu 24 godzin. Procesy wewnętrzne są częściowo zakłócone lub sparaliżowane. Istnieje niskie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
- **Priorytet średni** - Incydent prawdopodobnie nie wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT ze względu na brak symptomów działania z zewnątrz. Procesy wewnętrzne nie są sparaliżowane lub zakłócone w żadnym stopniu. Ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji nie występuje.

- Budowanie zespołów ds. bezpieczeństwa: Definicja ról, odpowiedzialności, umiejętności oraz ścieżek rozwoju dla członków zespołu bezpieczeństwa.

- Lista wymaganych kompetencji do omówienia na szkoleniu:

- Szef działu bezpieczeństwa (kierownik, dyrektor);
- Pełnomocnik ds. Bezpieczeństwa Informacji;
- Specjalista ds. Zarządzania Ryzykiem;
- Specjalista ds. Zgodności;
- Specjalista ds. Bezpieczeństwa Fizycznego;
- Architekt Systemów Bezpieczeństwa;
- Koordynator Programu Bezpieczeństwa;
- Analityk Bezpieczeństwa (II linia wsparcia);
- Inżynier ds. Bezpieczeństwa (II linia wsparcia);
- Administrator Systemów Bezpieczeństwa (II linia wsparcia);

4. Regulacje prawne i compliance:

- Zharmonizowanie działalności Podmiotu z imperatywami Ustawy o Krajowym Systemie Cyberbezpieczeństwa, z naciskiem na implementację procedur i protokołów zapewniających wytrzymałość infrastruktury informatycznej na potencjalne zagrożenia cyfrowe.

- Inicjacja, adaptacja, perpetuacja oraz ewolucja Systemu Zarządzania Bezpieczeństwem Informacji, skonstruowanego na fundamencie czterech norm określonych w paragrafie 20 Krajowego Ramienia Interoperacyjności, stanowiących kamień węgielny dla ochrony danych.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

- Egzekwowanie procedury tworzenia redundancji danych dziennikowych poprzez generowanie kopii zapasowych, które będą przechowywane przez okres minimalny dwóch lat, zgodnie z dyrektywą zawartą w paragrafie 21 Krajowego Ramienia Interoperacyjności.

- Implementacja kompleksowej agregacji logów (rejestrowanych zdarzeń) pochodzących z heterogenicznej gamy urządzeń, maszyn i aplikacji działających w ramach infrastruktury teleinformatycznej Podmiotu, umożliwiająca szczegółową analizę i audyt bezpieczeństwa.

- Integracja z zaawansowanym systemem zarządzania cyberbezpieczeństwem S46 (S46-react), celem optymalizacji procesów detekcji, reagowania i prewencji w zakresie incydentów bezpieczeństwa cyfrowego.

- Kodyfikacja programu regularnych audytów wewnętrznych i zewnętrznych, obejmujących spektrum standardów i regulacji (KRI, KSC, ISO, RODO).

- Monitorowanie zdarzeń systemowych w trybie ciągłym, poprzez wykorzystanie mechanizmów korelacji zdarzeń, umożliwiających identyfikację i interpretację wzorców aktywności sugerujących potencjalne scenariusze ataków cybernetycznych.

- Dostosowanie się do rozszerzonego zakresu wymagań wynikających z implementacji Dyrektywy NIS2, która wprowadza nowe, zaostrzone standardy w zakresie cyberbezpieczeństwa, wymagające od organizacji ponownej oceny i ulepszenia istniejących strategii ochrony danych.

- Wyznaczenie dedykowanego Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji, którego rola nie będzie interferować ani generować konfliktów interesów z innymi kluczowymi funkcjami w organizacji (np. Inspektorem Ochrony Danych, Informatykiem, Dyrektorem).

- Rekonfiguracja systemów informatycznych oraz protokołów pracy zdalnej w zgodzie ze zmienionymi standardami bezpieczeństwa, uwzględniającymi nowelizację Kodeksu Pracy, w celu zabezpieczenia integralności danych korporacyjnych w rozproszonym środowisku pracy.

- Realizacja oczekiwań organów nadzorczych w kontekście konstruowania oraz utrzymywania zaawansowanych systemów cyberbezpieczeństwa, zdolnych do przeciwdziałania współczesnym zagrożeniom w przestrzeni cyfrowej.

- Implementacja rygorystycznych protokołów ochrony danych osobowych, mających na celu eliminację ryzyka wycieków informacji, spowodowanych przez nieświadome bądź intencjonalne działania personelu organizacji.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

- Automatyzacja procesów aktualizacji oprogramowania w celu zapewnienia najwyższego poziom

5. Zarządzanie bezpieczeństwem w praktyce:

- Zrozumienie znaczenia typów licencji względem konieczności ich testowania:

- Licencje niewyłączne, w których udzielający licencji może zezwolić na korzystanie z utworu wielu osobom równocześnie, które nie muszą mieć formy pisemnej.
- Licencje wyłączne, spotykane głównie w przypadku oprogramowania pisanego na zamówienie (np. strona www), w tym przypadku zwykle umowa licencyjna wynika z umowy o dzieło, na podstawie której firma wykonująca oprogramowanie wykonuje zamówioną aplikację, umowa taka wymaga formy pisemnej pod rygorem nieważności.
- Sublicencja, w której licencjobiorca może udzielić dalszej licencji, pod warunkiem wszakże takiego upoważnienia w jego umowie licencyjnej.
- OEM, to programy sprzedawane wraz ze sprzętem komputerowym (przypisane do konkretnego komputera), po wymianie sprzętu na nowszy, nie można ich przenieść na nowy komputer tylko trzeba ponownie je zakupić.
- BOX, to programy, które można przenosić na kolejne komputery jednak pod warunkiem, że zawsze zainstalowany jest tylko na jednym komputerze. Legalny jest tylko program ostatnio zainstalowany.
- Open Source (otwarte oprogramowanie) to alternatywa dla Freeware (wolne oprogramowanie), którego celem jest istnienie swobodnego dostępu do oprogramowania dla wszystkich jego uczestników. Zapewnia swoim użytkownikom prawo do legalnego oraz darmowe.

Szkolenie powinno odbyć się w czasie nie krótszym niż 4 godziny robocze w ciągu jednego dnia z uwzględnieniem co najmniej 4 przerw po 15 minut. Po szkoleniu przewidziano 30 minut na pytania i odpowiedzi uczestników.

Z przeprowadzonego szkolenia Wykonawca musi przedstawić **listę obecności** z podpisami uczestników szkolenia.

Szkolenie musi być zakończone ankietą **oceniającą szkolenie**, jego przydatność, zakres przekazanych informacji, adekwatności przekazanych informacji do potrzeb uczestnika, formy prezentacji i komunikatywności prowadzącego szkolenie.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

5.2. Część 2.:

5.2.1Dostęp do platformy szkoleniowej dla pracowników Urzędu oraz jednostek podległych.

W ramach realizacji części 2. zamówienia Wykonawca zobowiązany będzie do zapewnienia pracownikom Zamawiającego **dostępu do platformy szkoleniowej** dla pracowników na okres 6 miesięcy oraz szkolenia dziedzinowego IT. Na platformie szkoleniowej (e-learningowej) zamieszczone będą różnorodne materiały szkoleniowe z zakresu cyberbezpieczeństwa. Materiały szkoleniowe muszą być przez Wykonawcę na bieżąco uzupełniane i aktualizowane, w związku z pojawianiem się nowych zagrożeń i podatności, nowych metod ochrony informacji i narzędzie do tego wykorzystywanych oraz zmieniającej się sytuacji geopolitycznej.

Udostępnienie platformy e-learningowej ma umożliwić pracownikom elastyczny dostęp do aktualnych informacji i standardowych praktyk w dogodnym dla nich czasie, co będzie sprzyjać skutecznej nauce, oraz poszerzenia wiedzy o inne tematy związane z cyberbezpieczeństwem.

Wykonawca zobowiąże się do udostępnienia platformy e-learningowej na niezmienionych warunkach technicznych, jakościowych i finansowych na co najmniej dwa kolejne okresy 6-miesięczne po zakończeniu realizacji zamówienia.

Liczba użytkowników platformy – 300

Termin udostępnienia platformy (wraz z całością materiału szkoleniowego) – najpóźniej 30 dni po podpisaniu umowy.

Okres udostępnienia platformy – 6 miesięcy bez konieczności automatycznego odnawiania subskrypcji

Platforma musi spełniać następujące wymagania:

Zawierać minimum 45 szkoleń, dostępnych w języku polskim (oraz w jęz. angielskim,

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

niemieckim, hiszpańskim, czeskim, słowackim, serbskim, chorwackim i włoskim), w postaci filmów i prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.

a) Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:

- ✓ Podstawy bezpiecznego internetu
- ✓ Bezpieczeństwo poczty
- ✓ Załączniki w poczcie elektronicznej
- ✓ Phishing
- ✓ Spyware/malware
- ✓ Bezpieczeństwo danych osobowych RODO/GDRP
- ✓ Bezpieczne hasła
- ✓ Menedżery haseł
- ✓ Bezpieczeństwo urządzeń mobilnych
- ✓ Uwierzytelnianie wieloskładnikowe (MFA)
- ✓ Bezpieczna praca zdalna
- ✓ Bezpieczna praca w biurze
- ✓ Sieci społeczne
- ✓ Zakupy w internecie

b) Użytkownicy powinni być podzieleni na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.

c) Łączny czas trwania wszystkich materiałów szkoleniowych powinien wynosić co najmniej 8 godzin.

2. Dedykowaną platformę phishingową pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail:

a) z linkiem prowadzącym do stronnym internetowej,

b) z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji,

c) z załącznikiem (szyfrowanym i niezaszyfrowanym) zawierającym potencjalnie niebezpieczny kod,

d) z załącznikiem w postaci dokumentu Word lub Excel zawierającym potencjalnie niebezpieczny kod.

W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.

3. dedykowaną platformę dostarczającą raporty obejmujące minimum:

a) status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

b) status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zwierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, jaka była platforma z jakiej wykonał tę akację oraz szczegółowe daty wykonania tych operacji.

W ramach świadczonej usługi usługodawca musi:
- przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników,
- zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi,
- zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,
- dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe,
- wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń (2 zmiany miesięcznie) lub liczby użytkowników (nie więcej niż 10% zmian w okresie trwania usługi).

Wymagania dodatkowe:
Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej. Dostawca platformy musi zapewnić całkowite usunięcie danych użytkowników po zakończeniu realizacji usługi. Wszystkie moduły (platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.
Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.
Do oferty należy załączyć oświadczenie usługodawcy o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001.

5.2.2. Szkolenie dziedzinowe IT Audytor wiodący ISO/IEC 27001:2022

Szkolenie dziedzinowe IT musi spełniać następujące wymagania:

- Forma szkolenia – stacjonarna w siedzibie realizatora szkolenia bądź zdalna na

wniosek zamawiającego

- Szkolenie powinno trwać co najmniej 5 dni

- Szkolenie zakończone powinno być egzaminem certyfikującym (Audytor wiodący ISO 27001:2022)

- Wymagane zagadnienia omawiane podczas szkolenia:

Co to jest system zarządzania bezpieczeństwem informacji?

Znaczenie i cel wdrażania SZBI

Korzyści z wdrożenia SZBI

Struktura, hierarchia i wzajemne powiązania pomiędzy dokumentami specyficznymi dla SZBI

Wymagania prawne i regulacyjne istotne dla bezpieczeństwa informacji

Terminologia

Rodzina normy serii ISO 27000

Wymagania normy PN-ISO/IEC 27001:2017:

1. Kontekst organizacji,
2. Przywództwo,
3. Planowanie w tym szacowanie ryzyka w bezpieczeństwie informacji i zarządzanie ryzykiem
4. Wsparcie,
5. Działania operacyjne,
6. Ocena wyników,
7. Doskonalenie

Analiza celów stosowania zabezpieczeń i zabezpieczeń ujętych w załączniku A do normy:

1. Zabezpieczenia organizacyjne

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

2. Bezpieczeństwo zasobów ludzkich

Analiza celów stosowania zabezpieczeń i zabezpieczeń ujętych w załączniku A do normy:

1. Zabezpieczenia fizyczne
2. Zabezpieczenia technologiczne

Metodyka audytu:

1. Cele, założenia i podstawowe pojęcia audytu (wg ISO 19011 i ISO/IEC 17021, ISO/IEC 27006 i ISO/IEC 27007)
2. Omówienie metodyki audytu i wyjaśnienie roli jej poszczególnych etapów
3. Planowanie audytu: prezentacja i omówienie technik planowania audytów
4. Przygotowanie się do audytu. Analiza dokumentacji klienta
5. Przeprowadzanie audytu. Omówienie technik.
6. Rozpoznawanie niezgodności: ćwiczenia oparte na faktycznych i fikcyjnych sytuacjach z przedsiębiorstw i urzędów
7. Raportowanie wyników audytu. Opracowanie dokumentacji poaudytowej

Przeprowadzanie audytów

1. Planowanie audytów ćwiczeniowych
2. Przygotowanie się do audytów
3. Opracowanie planu audytu, sporządzenie listy pytań kontrolnych, analiza dokumentacji

Akty prawne istotne z punktu widzenia bezpieczeństwa informacji:

1. Kodeks pracy
2. Ustawa o świadczeniu usług drogą elektroniczną
3. Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych
4. Ustawa o prawach autorskich i prawach pokrewnych

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Wymagania normy ISO/IEC 27001:2022 i zmiany wobec wydania z 2017 roku

Załącznik A i zmiany wobec wydania z 2017 roku

Wymagane jest aby szkolenie zostało zakończone egzaminem.

Po pomyślnie zdanym egzaminie uczestnik otrzyma certyfikat CQI/IRCA. Będzie on wysłany na adres e-mail w formie elektronicznej.

6. Harmonogram realizacji zamówienia

Terminy realizacji poszczególnych części:

Część 1.: W terminie do 30 dni od dnia podpisania umowy.

Część 2.: W terminie do 30 dni od dnia podpisania umowy.

7. Warunki płatności

Część 1. :

Płatność nastąpi w terminie do 30 dni od daty dostarczenia prawidłowo wystawionej FV, podstawą do wystawienia FV będzie dołączona lista obecności uczestników szkolenia.

Część 2 .:

2.1. Dostęp do platformy szkoleniowej dla pracowników Urzędu oraz jednostek podległych.

Płatność nastąpi w terminie do 30 dni od daty dostarczenia prawidłowo wystawionej FV, podstawą do wystawienia FV będzie potwierdzenie przekazania dostępu do platformy szkoleniowej.

2.2. Szkolenie dziedzinowe IT zakończone egzaminem z możliwością uzyskania certyfikacji ISO/IEC 27001:2022

Płatność w terminie do 30 dni od daty dostarczenia prawidłowo wystawionej FV, podstawą do wystawienia FV będzie dokument wykonawcy potwierdzający przystąpienie do egzaminu.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

8. Warunki udziału w postępowaniu

O udzielenie poszczególnych części zamówienia mogą ubiegać się Wykonawcy nie podlegający wykluczeniu i spełniający warunki udziału w postępowaniu, dotyczące **zdolności technicznej lub zawodowej**, którzy:

WYŁĄCZNIE dla części 1.:

1. W okresie ostatnich 3 lat wykonali lub wykonują co najmniej 1 szkolenie budujące i wzmacniające świadomość cyberzagrożeń dla co najmniej 10 uczestników.
2. Dysponują lub będą dysponować co najmniej 1 trenerem, który będzie uczestniczył w realizacji zamówienia i posiada:
   - wykształcenie wyższe,
   - certyfikat audytora wiodącego ISO/IEC 27001 w wersji 2007 lub nowszej lub inny certyfikat wymieniony w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999),
   - przeprowadził w okresie ostatnich trzech lat przed upływem terminu składania ofert przynajmniej 8 godzin (zegarowych) szkoleń na temat cyberbezpieczeństwa.

Na potwierdzenie spełnienia ww. warunków Wykonawca zobowiązany jest przedstawić dla części 1:

1.Wykaz usług zrealizowanych w okresie ostatnich trzech lat przed upływem terminu składania ofert – wzór wykazu stanowi **załącznik nr 4.** do niniejszego zapytania ofertowego wraz z dowodem potwierdzającym należyte wykonanie usługi.
2.Wykaz osób przeznaczonych do realizacji zamówienia publicznego, w szczególności odpowiedzialnych za przeprowadzenie szkoleń, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień i doświadczenia niezbędnego do wykonania zamówienia, a także kopiami dokumentów potwierdzającymi posiadane doświadczenie i certyfikaty – wzór wykazu stanowi **załącznik nr 3.** do niniejszego zapytania ofertowego.

Oferty Wykonawców nie spełniających ww. warunków będą podlegały odrzuceniu jako niezgodne z zapisem zapytania ofertowego.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Zamawiający zastrzega sobie prawo sprawdzania w toku oceny ofert wiarygodności przedstawionych przez Wykonawcę dokumentów, wykazów, danych i informacji.

9. Wykluczenie z udziału w postępowaniu

O udzielenie zamówienia nie może ubiegać się Wykonawca w stosunku do którego zachodzi którakolwiek z okoliczności, o których mowa w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2023 r. poz. 1497 z późn. zm.);
Zamawiający wykluczy z postępowania wykonawcę, który jest powiązany z Zamawiającym osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między beneficjentem lub osobami upoważnionymi do zaciągania zobowiązań w imieniu beneficjenta lub osobami wykonującymi w imieniu beneficjenta czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a wykonawcą, polegające w szczególności na:

1. uczestniczeniu w spółce, jako wspólnik spółki cywilnej lub spółki osobowej,
2. posiadaniu co najmniej 10% udziałów lub akcji,
3. pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
4. pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.

10. Sposób przygotowania oferty

1. Ofertę należy sporządzić na formularzu ofertowym stanowiącym **załącznik nr 1.** do niniejszego zapytania ofertowego.
2. Cena oferty musi być ceną ryczałtową, obejmować dowolną liczbę części zamówienia w całości i być podana w złotych polskich. Cena musi być rozbita na kwoty cząstkowe

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

stanowiące wynagrodzenie za realizację poszczególnych części zamówienia i edycji szkoleń.

3. Oferta winna być podpisana przez osobę/y upoważnione do reprezentowania Wykonawcy.
4. Oferta i załączone do niej oświadczenia i wymagane przez Zamawiającego, muszą być podpisane przez osoby upoważnione do reprezentowania Wykonawcy, wskazane we właściwym rejestrze bądź stosownym pełnomocnictwie. Dopuszcza się skan podpisanej oferty przygotowanej na wzorze zamieszczonym w ogłoszeniu bądź w formie elektronicznej lub w postaci elektronicznej za pomocą profilu zaufanego lub podpisu osobistego.
5. Termin związania ofertą wynosi 30 dni.
6. Wykonawca informuje Zamawiającego o informacjach zawartych w ofercie stanowiących tajemnicę przedsiębiorstwa.

11. Wymagane dokumenty

Wraz z ofertą części 1 Wykonawca jest zobowiązany złożyć dokumenty potwierdzające należytą realizację zamówień wymienionych w wykazie usług oraz certyfikat potwierdzający posiadanie przez audytora uprawnienia wymienione w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
Do oferty musi zostać załączony wykaz usług stanowiący załącznik nr 4. - Oświadczenie o braku powiązań z Zamawiającym i braku podstaw do wykluczenia oraz załącznik nr 3 – Wykaz osób

12. Miejsce i termin składania ofert:

1. Ofertę wraz z załącznikami należy złożyć za pośrednictwem portalu Baza Konkurencyjności – https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl
   w terminie do dnia 23.10.2024 r. do godziny 10.00

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

2. O terminowym złożeniu oferty decyduje data złożenia oferty za pośrednictwem portalu Baza Konkurencyjności.
3. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
4. Oferta winna być sporządzona w języku polskim pod rygorem nieważności. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem przysięgłym na język polski.
5. **Zamawiający nie dopuszcza innego sposobu składania ofert niż za pośrednictwem portalu Baza Konkurencyjności**. Niespełnienie tego wymogu oznacza niezgodność oferty z Zapytaniem. Oferty złożone w inny sposób zostaną odrzucone przez Zamawiającego.

13. Kryteria wyboru oferty

1. Przy wyborze oferty Zamawiający będzie się kierował następującym kryterium:

   Część 1 :

   cena brutto – 70%

   doświadczenie trenera – 30%

   Ocena w kryterium cena nastąpi w oparciu o poniżej określony wzór:

   Ilość punktów = C_{min}/C_{wn} x 100 pkt x waga kryterium

   Gdzie:

   C_{min} – cena minimalna spośród zaproponowanych cen ofertowych,

   C_{wn} – cena zaproponowana przez wykonawcę n

   Kryterium doświadczenie trenera. Ocena nastąpi wg punktów przyznanych za ilość przeprowadzonych szkoleń w obszarze cyberbezpieczeństwa.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Ilość punktów z tytułu przeprowadzonych szkoleń:

1 szkolenie – przeprowadził w okresie ostatnich trzech lat przed upływem terminu składania ofert przynajmniej 8 godzin zegarowych szkoleń w okresie ostatnich 3 lat na temat cyberbezpieczeństwa – 0 pkt

2 – przeprowadził w okresie ostatnich trzech lat przed upływem terminu składania ofert przynajmniej 2 szkolenia w okresie ostatnich 3 lat na temat cyberbezpieczeństwa bez względu na ilość godzin - 5 pkt

3 – przeprowadził w okresie ostatnich trzech lat przed upływem terminu składania ofert przynajmniej 3 szkolenia w okresie ostatnich 3 lat na temat cyberbezpieczeństwa bez względu na ilość godzin - 10 pkt

4 – przeprowadził w okresie ostatnich trzech lat przed upływem terminu składania ofert przynajmniej 4 szkolenia w okresie ostatnich 3 lat na temat cyberbezpieczeństwa bez względu na ilość godzin - 15 pkt

5 – przeprowadził w okresie ostatnich trzech lat przed upływem terminu składania ofert przynajmniej 5 szkoleń w okresie ostatnich 3 lat na temat cyberbezpieczeństwa bez względu na ilość godzin - 20 pkt

6 – przeprowadził w okresie ostatnich trzech lat przed upływem terminu składania ofert przynajmniej 6 szkoleń w okresie ostatnich 3 lat na temat cyberbezpieczeństwa bez względu na ilość godzin - 25 pkt

7 i więcej – przeprowadził w okresie ostatnich trzech lat przed upływem terminu składania ofert przynajmniej 7 szkoleń w okresie ostatnich 3 lat na temat cyberbezpieczeństwa bez względu na ilość godzin - 30 pkt

Zamówienie w zakresie części 1 zostanie udzielone wykonawcy który uzyska najwyższą ilość punktów (cena + doświadczenie trenera) spośród wszystkich ważnych złożonych ofert.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | CENTRUM PROJEKTÓW POLSKA CYFROWA

Część 2 :

cena za udostępnienie platformy – 50%

obliczoną zgodnie z poniżej określonym wzorem:

Ilość punktów cena za udostępnienie platformy =

$C\ 1 = C_{min\ A} / C_{wn\ A}$ x 100 pkt x 50%

Gdzie:

C_{min} – cena minimalna spośród zaproponowanych cen ofertowych,

C_{wn} – cena zaproponowana przez wykonawcę n

A – Cena za udostępnienie platformy szkoleniowej

cena za szkolenie dziedzinowe IT – 50%

obliczoną zgodnie z poniżej określonym wzorem:

Ilość punktów cena za udostępnienie platformy =

$C\ 2 = C_{min\ B} / C_{wn\ B}$ x 100 pkt x 50%

Gdzie:

C_{min} – cena minimalna spośród zaproponowanych cen ofertowych,

C_{wn} – cena zaproponowana przez wykonawcę n

B – Cena za szkolenie dziedzinowe IT

Zamówienie w zakresie części 2 zostanie udzielone wykonawcy który uzyska najwyższą ilość punktów: C1 +C 2 spośród wszystkich ważnych złożonych ofert.

2. W sytuacji gdy cena najkorzystniejszej oferty będzie znacząco przewyższała środki zabezpieczone przez Zamawiającego w budżecie, Zamawiający zastrzega sobie możliwość przeprowadzenia dodatkowych negocjacji z Wykonawcą który złoży najkorzystniejszą ofertę.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

14. Kontakt z Zamawiającym

1. Komunikacja z zamawiającym o udzielenie zamówienia, w tym składanie ofert, wymiana informacji oraz przekazywanie dokumentów i oświadczeń odbywa się pisemnie za pomocą Bazy Konkurencyjności.
2. Po stronie Zamawiającego osobą do kontaktów w sprawie zamówienia jest:
   Sylwia Mróz – kierownik projektu, e-mail: s.mroz@um.malbork.pl, tel. 55 629 04 51
   Anita Kluczyk -Wąsik – zastępca kierownika projektu, e-mail: a.kluczyk@um.malbork.pl, tel. 55 629 04 86
   Grzegorz Koniszewski – koordynator techniczny, e-mail: g.koniszewski@um.malbork.pl,
   tel. 55 629 04 03
   Maciej Gadowski – koordynator techniczny, e-mail: m.gadowski@um.malbork.pl, tel. 55 629 04 20
3. W tytule wiadomości należy wskazać numer zapytania ofertowego – 1/WPR/2024

15. Wyjaśnienia oraz uzupełnienia do oferty

1. W toku badania ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonej oferty, treści oświadczeń, dokumentów, pełnomocnictw i ich uzupełnienia
2. Jeżeli zaoferowana cena będzie rażąco niska (30%) w stosunku do przedmiotu zamówienia lub będzie budziła wątpliwości co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi przez Zamawiającego lub wynikającymi z odrębnych przepisów, Zamawiający zwróci się do wykonawcy o udzielenie wyjaśnień, w tym złożenie dowodów dotyczących wyliczenia ceny. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu będzie spoczywać na Wykonawcy.
3. Zamawiający odrzuci ofertę Wykonawcy, który nie udzieli wyjaśnień, o których mowa

powyżej lub jeżeli dokonana ocena tych wyjaśnień wraz ze złożonymi dowodami potwierdzi, że zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia.

4. Zamawiający wyjaśni i poprawi w formularzu ofertowym:

oczywiste omyłki pisarskie, oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek, inne omyłki polegające na niezgodności oferty z opisem zawartym w zapytaniu ofertowym niepowodujące istotnych zmian w treści oferty. Poprawienie przez Zamawiającego oczywistych omyłek pisarskich oraz rachunkowych i konsekwencji rachunkowych dokonanych poprawek nie wymaga uzyskania zgody wykonawcy. Wykonawca może nie wyrazić zgody na poprawienie przez zamawiającego innych omyłek polegających na niezgodności oferty z opisem zawartym w zapytaniu ofertowym niepowodujące istotnych zmian w treści oferty. Brak zgody Wykonawca musi wnieść na piśmie w wyznaczonym przez Zamawiającego terminie.

5. Zamawiający zastrzega sobie prawo do unieważnienia postępowania bez dokonania wyboru żadnej z ofert, na każdym etapie prowadzonego postępowania. Z tytułu unieważnienia postępowania, Wykonawcy nie przysługuje żadne roszczenie wobec Zamawiającego.
6. W przypadku gdy wybrany Wykonawca odstąpi od podpisania umowy z Zamawiającym, możliwe jest podpisanie przez Zamawiającego umowy z kolejnym Wykonawcą, który w postępowaniu uzyskał kolejną najwyższą liczbę punktów.

16. Klauzula informacyjna RODO

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o danych) (Dz. U. UE L119 z dnia 4 maja 2016 r., str. 1; zwanym dalej „RODO") informujemy, że:

1. Administratorem Pani/Pana danych osobowych jest Miasto Malbork z siedzibą w Malborku 82-200, Plac Słowiański 5.
2. Administrator wyznaczył Inspektora Danych Osobowych, z którym można się kontaktować pod adresem e-mail: iod@um.malbork.pl, pod nr tel. +48 55 629 04 03 lub pisemnie na adres siedziby, wskazany powyżej.
3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z przedmiotowym postępowaniem o udzielenie zamówienia publicznego, prowadzonym w trybie zapytania ofertowego
4. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja zapytania ofertowego;
5. Pani/Pana dane osobowe będą przechowywane przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia;
6. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest związany z udziałem w postępowaniu o udzielenie zamówienia;
7. W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;
8. Posiada Pani/Pan:
   8.1. na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących (w przypadku, gdy skorzystanie z tego prawa wymagałoby po stronie Administratora niewspółmiernie dużego wysiłku może zostać Pani/Pan zobowiązana do wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia albo sprecyzowanie nazwy lub daty zakończonego postępowania);
   8.2. Na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia ani zmianą postanowień umowy oraz nie może naruszać integralności protokołu oraz jego załączników);

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

8.3. Na podstawie art. 18 RODO prawo żądania od Administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem okresu trwania postępowania o udzielenie zamówienia publicznego lub konkursu oraz przypadków, o których mowa w art. 18 ust. 2 RODO (prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego);

8.4. Prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

9. Nie przysługuje Pani/Panu:

9.1. w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;

9.2. prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

9.3. na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO;

10. Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Pana danych osobowych przez administratora. Organem właściwym dla przedmiotowej skargi jest Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

Załączniki:

1. Formularz oferty (załącznik nr 1)
2. Oświadczenie o braku powiązań z Zamawiającym i braku podstaw do wykluczenia (załącznik nr 2)
3. Wykaz osób (załącznik nr 3)
4. Wykaz usług (załącznik nr 4)

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa