|  |  |
| --- | --- |
| Nr postępowania: **RGKiM.271.12.2022.WJa** | ***Załącznik nr 1 do SWZ*** |

**Zamawiający:**

**Gmina Miasta Puck**

**ul. 1 Maja 13, 84-100 Puck**

**Formularz ofertowy**

**Wykonawca:**

|  |  |
| --- | --- |
| Pełna nazwa Wykonawcy /Wykonawców występujących wspólnie |  |
| NIP |  |
| REGON |  |
| KRS/CEiDG |  |
| Adres siedziby Wykonawcy |  |
| Adres do korespondencji |  |
| Telefon kontaktowy |  |
| E-mail |  |
| Osoba upoważniona do reprezentowania Wykonawcy | *(imię i nazwisko, stanowisko/podstawa do reprezentacji)* |

Ubiegając się o udzielenie zamówienia publicznego na roboty budowlane dla zadania pn.

**Usługi z zakresu cyberbezpieczeństwa dla Gminy Miasta Puck w ramach projektu grantowego „Cyfrowa Gmina”. W podziale na części:**

 **Cz. nr 1.** **Usługa wykonania diagnozy cyberbezpieczeństwa dla Urzędu Miasta Puck.**

 **Cz. nr 2. Usługa szkolenia pracowników Urzędu Miasta Puck z zakresu cyberbezpieczeństwa.**

1. Oferuję/emy **zrealizowanie przedmiotu zamówienia za**:
2. Cz. nr 1 Usługa wykonania diagnozy cyberbezpieczeństwa dla Urzędu Miasta Puck.

|  |  |
| --- | --- |
| cenę netto: | ………………………………zł |
| podatek VAT: | ………………………………zł |
| **cenę brutto:** | ………………………………zł |

1. Cz. nr 2 Usługa szkolenia pracowników Urzędu Miasta Puck z zakresu cyberbezpieczeństwa.

|  |  |
| --- | --- |
| cenę netto: | ………………………………zł |
| podatek VAT: | ………………………………zł |
| **cenę brutto:** | ………………………………zł |

Termin rozpoczęcia prac liczony będzie od dnia podpisania umowy.

Oświadczam/y, że przedmiot zamówienia zostanie wykonany w terminach określonych w SWZ.

Oświadczam/y, że zapoznałem/liśmy się z wymaganiami Zamawiającego, dotyczącymi przedmiotu zamówienia, zamieszczonymi w SWZ wraz z załącznikami i nie wnoszę/wnosimy do nich żadnych zastrzeżeń.

Oświadczam/y, że uważam/y się związanym/i niniejszą ofertą przez okres 30 dni od upływu terminu składania ofert.

Oświadczam/y, że zrealizuje/my zamówienie zgodnie z SWZ, Szczegółowym Opisem Przedmiotu Zamówienia i wzorem umowy.

Oświadczam/y, że informacje znajdujące się na stronach od ……… do ……… stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i zastrzegamy, że nie mogą być one udostępniane. Informacje i dokumenty zawarte na pozostałych stronach są jawne.

W przypadku wybrania mojej/naszej oferty jako najkorzystniejszej zobowiązuję/jemy się do wniesienia zabezpieczenia należytego wykonania umowy w wysokości **5%** **ceny ofertowej brutto** w formie …………………………………………

Oświadczam/y, że w razie wybrania mnie/nas na Wykonawcę niniejszego zamówienia zobowiązuje/jemy się do podpisania umowy na warunkach określonych we wzorze umowy.

Oświadczam/y, że wypełniłem/liśmy, a w przypadku danych przekazanych w przyszłości – wypełnię/imy – obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem/liśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu, a w przypadku wyboru mojej/naszej oferty, również w związku z zawarciem i wykonaniem umowy o zamówienie.

Oświadczam, że jestem przedsiębiorcą *(zaznaczyć odpowiednie)*:

* Mikroprzedsiębiorstwem *(przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 mln euro)*
* Małym *(przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 mln euro)*
* Średnim *(przedsiębiorstwo, które nie jest mikroprzedsiębiorstwem ani małym przedsiębiorstwem i które zatrudnia mniej niż 250 osób i którego roczny obrót nie przekracza 50 mln euro lub roczna suma bilansowa nie przekracza 43 mln euro)*
* Dużym *(przedsiębiorstwo, które nie jest mikroprzedsiębiorstwem, małym ani średnim przedsiębiorstwem)*

W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia powyższy punkt należy powielić dla każdego Wykonawcy ze wskazaniem nazwy Wykonawcy.

Oświadczam/y, że *(zaznaczyć odpowiednie)*:

* nie zamierzam/y powierzyć Podwykonawcom wykonania części zamówienia;
* powierzę/powierzymy niżej wymienione części niniejszego zamówienia Podwykonawcom:

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

*(nazwa części zadania / zakres prac powierzony Podwykonawcom oraz dane firmy Podwykonawcy – jeżeli są już znane)*

Dokumenty lub oświadczenia do wykorzystania przez Zamawiającego *(które znajdują się w posiadaniu Zamawiającego lub można je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych)*:

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa dokumentu | Tytuł/nr postępowania, adres strony internetowej |
|  |  |  |
|  |  |  |

Oświadczam/y, że wykonam/y zamówienie zgodnie z SWZ, Szczegółowym Opisem Przedmiotu Zamówienia oraz biorąc pod uwagę, że:

**Wykonawca może opisać przedmiot zamówienia przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, jeżeli nie można opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób, a wskazaniu takiemu towarzyszyć będą wyrazy „lub równoważny”. Jeżeli Wykonawca opisze przedmiot zamówienia w sposób, o którym mowa wyżej, wówczas wskaże w opisie przedmiotu zamówienia także kryteria stosowane w celu oceny równoważności.**

Informuje/my, że wybór mojej/naszej oferty *(zaznaczyć odpowiednie)*:

* nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług;
* będzie prowadzić do powstania u Zamawiającego ww. obowiązku dla następujących towarów lub usług:

…………………………………………………………………………………………………………………………………………………………………………………………………………

*(należy podać rodzaj towaru lub usługi wraz z wartością towaru lub usługi (bez podatku) oraz stawkę podatku (zgodnie z wiedzą Wykonawcy), która będzie miała zastosowanie)*

Składam/yofertęna ……… stronach.

Wraz z ofertą składam/y następujące oświadczenia i dokumenty:

………………………………………………………………………………………………………………………………………………………………………………………………………………………………

|  |  |
| --- | --- |
| **Miejscowość i data** | **Podpis Wykonawcy lub osoby uprawnionej do reprezentowania Wykonawcy*****Wymagany elektroniczny podpis kwalifikowany lub podpis zaufany lub podpis osobisty*** |
| ……………………………………… |  |

|  |  |
| --- | --- |
| Nr postępowania: **RGKiM.271.12.2022.WJa** | ***Załącznik nr 2 do SWZ******składany wraz z ofertą*** |

|  |  |
| --- | --- |
| **Zamawiający** | **Wykonawca** |
| **Gmina Miasta Puck**ul. 1 Maja 1384-100 Puck | ………………………………………………………………………………………………………………………………………………………………………………………*(pełna nazwa, adres)* |

**Oświadczenie wstępne Wykonawcy**

**o braku podstaw do wykluczenia oraz spełnieniu warunków udziału w postępowaniu**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn.

**Usługi z zakresu cyberbezpieczeństwa dla Gminy Miasta Puck w ramach projektu grantowego „Cyfrowa Gmina”. W podziale na części:**

**1. Usługa wykonania diagnozy cyberbezpieczeństwa dla Urzędu Miasta Puck.**

**2. Usługa szkolenia pracowników Urzędu Miasta Puck z zakresu cyberbezpieczeństwa.**

prowadzonego przez **Gminę Miasta Puck** składam następujące oświadczenia:

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie **art. 108 ust. 1** ustawy Pzp.

2.Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie **art. 109 ust. 1 pkt 4** ustawy Pzp.

3.Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art.……… ustawy Pzp *(jeżeli dotyczy, podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2 i 5 lub art. 109 ust. 1 pkt 4 ustawy Pzp)*. Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjąłem następujące środki naprawcze:…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

4.Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie 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. poz. 835)*[[1]](#footnote-1)*

5.Oświadczam, że spełniam warunki udziału w postępowaniu określone przez Zamawiającego w SWZ do zamówienia nr RGKiM.271.12.2022.WJa.

6.Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawieniu informacji.

|  |  |
| --- | --- |
| **Miejscowość i data** | **Podpis Wykonawcy lub osoby uprawnionej do reprezentowania Wykonawcy*****Wymagany elektroniczny podpis kwalifikowany lub podpis zaufany lub podpis osobisty*** |
| ……………………………………… |  |

|  |  |
| --- | --- |
| Nr postępowania: **RGKiM.271.12.2022.WJa** | ***Załącznik nr 2a do SWZ******składany wraz z ofertą (jeżeli dotyczy)*** |

|  |  |
| --- | --- |
| **Zamawiający** | **Podmiot udostępniający zasoby** |
| **Gmina Miasta Puck**ul. 1 Maja 1384-100 Puck | ………………………………………………………………………………………………………………………………………………………………………………………*(pełna nazwa, adres)* |

**Oświadczenie wstępne Podmiotu udostępniającego zasoby**

**o braku podstaw do wykluczenia oraz spełnieniu warunków udziału w postępowaniu**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn.

**Usługi z zakresu cyberbezpieczeństwa dla Gminy Miasta Puck w ramach projektu grantowego „Cyfrowa Gmina”. W podziale na części:**

**1. Usługa wykonania diagnozy cyberbezpieczeństwa dla Urzędu Miasta Puck.**

**2. Usługa szkolenia pracowników Urzędu Miasta Puck z zakresu cyberbezpieczeństwa.**

prowadzonego przez **Gminę Miasta Puck** składam następujące oświadczenia:

1.Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie **art. 108 ust. 1** ustawy Pzp.

2.Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie **art. 109 ust. 1 pkt 4** ustawy Pzp.

3.Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art.……… ustawy Pzp *(jeżeli dotyczy, podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2 i 5 lub art. 109 ust. 1 pkt 4 ustawy Pzp)*. Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjąłem następujące środki naprawcze:…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

4.Oświadczam, że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie 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. poz. 835)*[[2]](#footnote-2)*

5.Oświadczam, że spełniam warunki udziału w postępowaniu określone przez Zamawiającego w SWZ do zamówienia nr RGKiM.271.12.2022.WJa.

6.Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawieniu informacji.

|  |  |
| --- | --- |
| **Miejscowość i data** | **Podpis Podmiotu udostępniającego zasoby lub osoby uprawnionej do reprezentowania Podmiotu*****Wymagany elektroniczny podpis kwalifikowany lub podpis zaufany lub podpis osobisty*** |
| ……………………………………… |  |

|  |  |
| --- | --- |
| Nr postępowania: **RGKiM.271.12.2022.WJa** | ***Załącznik nr 3 do SWZ******składany wraz z ofertą (jeżeli dotyczy)*** |

|  |  |
| --- | --- |
| **Zamawiający** | **Podmiot udostępniający zasoby** |
| **Gmina Miasta Puck**ul. 1 Maja 1384-100 Puck | …………………………………………………………………………………………………………………………*(pełna nazwa, adres)* |

**Zobowiązanie Podmiotu udostępniającego zasoby**

**do oddania do dyspozycji Wykonawcy niezbędnych zasobów na potrzeby realizacji zamówienia**

W imieniu:

………………………………………………………………………………………………………………….

*(pełna nazwa , adres podmiotu, na zasobach którego polega Wykonawca)*

zobowiązuje się do oddania swoich zasobów:

………………………………………………………………………………………………………………….

*(określenie zasobu – np. wiedza i doświadczenie, potencjał kadrowy, potencjał ekonomiczno-finansowy)*

do dyspozycji Wykonawcy:

………………………………………………………………………………………………………………….

*(pełna nazwa, adres Wykonawcy)*

Przy wykonaniu zamówienia pn. **Usługi z zakresu cyberbezpieczeństwa dla Gminy Miasta Puck w ramach projektu grantowego „Cyfrowa Gmina”. W podziale na części:**

**1. Usługa wykonania diagnozy cyberbezpieczeństwa dla Urzędu Miasta Puck.**

**2. Usługa szkolenia pracowników Urzędu Miasta Puck z zakresu cyberbezpieczeństwa.**

Jednocześnie oświadczam, że:

1. udostępniam Wykonawcy ww. zasoby, w następującym zakresie:

………………………………………………………………………………………………………………

sposób wykorzystania udostępnianych przeze mnie zasobów będzie następujący:

………………………………………………………………………………………………………………

charakter stosunku łączącego mnie z Wykonawcą będzie następujący:

………………………………………………………………………………………………………………

zakres mojego udziału przy wykonywaniu zamówienia będzie następujący:

………………………………………………………………………………………………………………

okres mojego udziału przy wykonywaniu zamówienia będzie następujący:

………………………………………………………………………………………………………………

|  |  |
| --- | --- |
| **Miejscowość i data**…………………………………… | **Podpis Podmiotu udostępniającego zasoby lub osoby uprawnionej do reprezentowania Podmiotu udostępniającego zasoby*****Wymagany elektroniczny podpis kwalifikowany lub podpis zaufany lub podpis osobisty*** |

|  |  |
| --- | --- |
| Nr postępowania: **RGKiM.271.12.2022.WJa** | ***Załącznik nr 4 do SWZ******składany wraz z ofertą (jeżeli dotyczy)*** |

|  |  |
| --- | --- |
| **Zamawiający** | **Wykonawcy w imieniu których składane jest oświadczenie** |
| **Gmina Miasta Puck**ul. 1 Maja 1384-100 Puck | 1. ………………………………………………………………………………………………………………………2. ………………………………………………………………………………………………………………………3. ………………………………………………………………………………………………………………………*(pełna nazwa, adres)* |

**Oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia**

**(podział zadań Wykonawców)**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn.

**Usługi z zakresu cyberbezpieczeństwa dla Gminy Miasta Puck w ramach projektu grantowego „Cyfrowa Gmina”. W podziale na części:**

**1. Usługa wykonania diagnozy cyberbezpieczeństwa dla Urzędu Miasta Puck.**

**2. Usługa szkolenia pracowników Urzędu Miasta Puck z zakresu cyberbezpieczeństwa.**

prowadzonego przez **Gminę Miasta Puck**, działając jako pełnomocnik Wykonawców, w imieniu których składane jest oświadczenie, oświadczam co następuje:

1. następujące usługi:

………………………………………………………………………………………………………………

wykona Wykonawca:

………………………………………………………………………………………………………………

1. następujące usługi:

………………………………………………………………………………………………………………

wykona Wykonawca:

………………………………………………………………………………………………………………

|  |  |
| --- | --- |
| **Miejscowość i data** | **Podpis osoby uprawnionej do reprezentowania Wykonawców wspólnie ubiegających się o udzielenie zamówienia*****Wymagany elektroniczny podpis kwalifikowany lub podpis zaufany lub podpis osobisty*** |
| ……………………………………… |  |
| Nr postępowania: **RGKiM.271.12.2022.WJa** | ***Załącznik nr 5 do SWZ******składany na wezwanie Zamawiającego*** |

|  |  |
| --- | --- |
| **Zamawiający** | **Wykonawca** |
| **Gmina Miasta Puck**ul. 1 Maja 1384-100 Puck | ………………………………………………………………………………………………………………………………………………………………………………………*(pełna nazwa, adres)* |

**Oświadczenie Wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy Pzp**

**o przynależności lub braku przynależności do tej samej grupy kapitałowej**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn.

**Usługi z zakresu cyberbezpieczeństwa dla Gminy Miasta Puck w ramach projektu grantowego „Cyfrowa Gmina”. W podziale na części:**

**1. Usługa wykonania diagnozy cyberbezpieczeństwa dla Urzędu Miasta Puck.**

**2. Usługa szkolenia pracowników Urzędu Miasta Puck z zakresu cyberbezpieczeństwa.**

prowadzonego przez **Gminę Miasta Puck** oświadczam, że *(zaznaczyć odpowiednie)*:

* **nie należymy do tej samej grupy kapitałowej**, o której mowa w art. 108 ust. 1 pkt 5 ustawy Pzp, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2020 r., poz. 1076 ze zm.) z innym Wykonawcą, który złożył odrębną ofertę / ofertę częściową;
* **należymy do tej samej grupy kapitałowej**, o której mowa w art. 108 ust. 1 pkt 5 ustawy Pzp, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2020 r., poz. 1076 ze zm.) co Wykonawca ……………………………………………*(podać nazwę)*, który złożył odrębną ofertę / ofertę częściową i przedkładam w załączeniu dokumenty i/lub informacje potwierdzające przygotowanie oferty / oferty częściowej niezależnie od Wykonawcy ……………………………………………*(podać nazwę)* będącego członkiem tej samej grupy kapitałowej:

…………………………………………………………………………………………………………

Na potwierdzenie powyższego załączam następujące dokumenty:

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

|  |  |
| --- | --- |
| **Miejscowość i data** | **Podpis Wykonawcy lub osoby uprawnionej do reprezentowania Wykonawcy*****Wymagany elektroniczny podpis kwalifikowany lub podpis zaufany lub podpis osobisty*** |
| ……………………………………… |  |

|  |  |
| --- | --- |
| Nr postępowania: **RGKiM.271.12.2022.WJa** | ***Załącznik nr 7 do SWZ*** |

**Szczegółowy Opis Przedmiotu Zamówienia (OPZ)**

dla zadania pn.

**Usługi z zakresu cyberbezpieczeństwa dla Gminy Miasta Puck w ramach projektu grantowego „Cyfrowa Gmina”.**

**w podziale na części:**

**1. Usługa wykonania diagnozy cyberbezpieczeństwa dla Urzędu Miasta Puck.**

**2. Usługa szkolenia pracowników Urzędu Miasta Puck z zakresu cyberbezpieczeństwa.**

Część 1:

Usługa wykonania diagnozy cyberbezpieczeństwa dla Urzędu Miasta Puck

1. Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)

• wyznaczenie osoby do kontaktu – Art. 21 KSC

• przekazanie danych osoby wyznaczonej – Art. 22 pkt 5) KSC

• zapewnienie zarządzania incydentem – Art. 22 pkt 1) KSC

• zgłaszanie incydentu – Art. 22 pkt 2) Art. 23 KSC

• zapewnienie obsługi incydentu – Art. 22 pkt 3) KSC

• zapewnienie dostępu do wiedzy – Art. 22 pkt 4) KSC

• opracowanie, ustanowienie i wdrożenie SZBI – Par. 20 KRI

• monitorowanie i przegląd SZBI – Par. 20 KRI

• doskonalenie SZBI – Par. 20 KRI

• aktualizowanie regulacji wewnętrznych – Par. 20 pkt 1) KRI

• inwentaryzacja sprzętu i oprogramowania – Par. 20 pkt 2) KRI

• przeprowadzanie okresowych analiz ryzyka – Par. 20 pkt 3) KRI

• postępowanie z ryzykiem – Par. 20 pkt 3) KRI

• zarządzanie uprawnieniami – Par. 20 pkt 4), 5) KRI

• szkolenia i uświadamianie – Par. 20 pkt 6) KRI

• monitorowanie dostępu do informacji – Par. 20 pkt 7) a), b) KRI

• monitorowanie nieautoryzowanych zmian – Par. 20 pkt 7) b) KRI

• zabezpieczenie nieautoryzowanego dostępu – Par. 20 pkt 7) c) KRI

• ustanowienie zasad bezpiecznej pracy mobilnej – Par. 20 pkt 8) KRI

• zabezpieczenie informacji przed nieuprawnionym ujawnieniem – Par. 20 pkt 9) KRI

• zabezpieczenie informacji przed nieuprawnioną modyfikacją – Par. 20 pkt 9) KRI

• zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem – Par. 20 pkt 9) KRI

• zawieranie w umowach serwisowych zapisów o bezpieczeństwie – Par. 20 pkt 10) KRI

• ustalenie zasad postępowania z informacjami w celu minimalizacji kradzieży informacji i środków

przetwarzania – Par. 20 pkt 11) KRI

• aktualizowanie oprogramowania – Par. 20 pkt 12) a) KRI

• minimalizowanie ryzyka utraty informacji w wyniku awarii systemu – Par. 20 pkt 12) b) KRI

• ochrona systemu przed błędami – Par. 20 pkt 12) c) KRI

• stosowanie mechanizmów kryptograficznych w systemach – Par. 20 pkt 12) d) KRI

• zapewnienie bezpieczeństwa plików systemowych – Par. 20 pkt 12) e) KRI

• zarządzanie podatnościami systemów – Par. 20 pkt 12) f), g) KRI

• kontrola zgodności systemów z regulacjami – Par. 20 pkt 12) h) KRI

• zapewnienie audytu bezpieczeństwa informacji nie rzadziej niż raz na rok – Par. 20 pkt 14) KRI

2. Ocena wybranych aspektów bezpieczeństwa systemów informatycznych

• dokumentacja potwierdzająca wykonane działania wskazanego w ustawie

• opis identyfikacji systemu informacyjnego wspierającego zadanie publiczne

• dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne

• dokumentacja procesu zarządzania incydentami

• aspekty techniczne do weryfikacji

3. Ocena dojrzałości wybranych procesów bezpieczeństwa

• ochrona przed kodem szkodliwym

• ochrona sieci i połączeń

• ochrona urządzeń końcowych

• zarządzanie tożsamością i autoryzacją dostępu

• ochrona fizyczna systemów IT

• bezpieczeństwo urządzeń drukujących

• zarządzanie podatnościami

4. Opracowanie raportu z audytu oraz uzupełnienie arkusza do oceny.

Testy penetracyjne infrastruktury sieciowej

1. Przedstawienie założeń Audytu

Audyt wykonywany będzie w sposób manualny oraz automatyczny za pomocą specjalistycznych narzędzi oraz własnych skryptów przygotowanych na podstawie wiedzy i doświadczeń. Testy zostaną przeprowadzone w oparciu o OSSTMM (Open Source Security Testing Methodology Manual).

2. Weryfikacja dokumentacji sieci, topologii sieci, kluczowych elementów sieci

3. Skanowanie sieci – rekonesans sieci

Sprawdzenie jakie hosty są w sieci widoczne, ile ich jest, usługi jakie są uruchomione na hostach, jakie systemy operacyjne działają na wykrytych hostach. W szczególności ten etap polega na:

• skanowaniu sieci w poszukiwaniu wszystkich podłączonych hostów

• wykryciu czy jest dostęp do innych podsieci z danej podsieci

• wykryciu usług działających na hostach podłączonych do sieci

• wykryciu podatności na wybranych hostach w sieci

4. Skanowanie będzie powtórzone dla każdej wskazanej przez zamawiającego sieci

Przeprowadzenie skanowania w prawidłowo działającej sieci nie powinno mieć negatywnego wpływu na działanie sieci. Po przeskanowaniu sieci wraz z Zamawiającym zostanie wybrana pula hostów do dalszego badania.

5. Skanowanie najistotniejszych hostów w sieci (serwery, kluczowe stacje końcowe, kamery, rejestratory), które zostały wybrane na podstawie wcześniejszej analizy

• weryfikacja występowania luk bezpieczeństwa dla konkretnych usług

• w zależności od wykrytej usługi weryfikacja haseł

• weryfikacja dostępu użytkowników do odpowiednich usług

• weryfikacja możliwości dostępu do usługi

• weryfikacja luk bezpieczeństwa w systemie operacyjnym

• weryfikacja luk bezpieczeństwa w oprogramowaniu firm trzecich

6. Sprawdzenie domyślnych haseł dla najistotniejszych hostów w sieci (serwery, bramy, switche, access point), które zostały wybrane na podstawie wcześniejszej analizy

• weryfikacja haseł w usługach umożliwiających logowanie

7. Sprawdzenie możliwości wylistowania użytkowników oraz zdobycia haseł

8. Weryfikacja możliwości uzyskania dostępu do zasobów współdzielonych

9. Weryfikacja zabezpieczeń urządzeń sieciowych

• badanie odporności switchy na ataki sieciowe

• weryfikacja zabezpieczeń monitoringu wizyjnego

10. Testy sieci bezprzewodowej oraz weryfikacja zabezpieczeń sieci bezprzewodowej

• weryfikacja pod kątem dostępu

• weryfikacja pod kątem zabezpieczeń

• wykrycie możliwości przechwycenia haseł

• w przypadku przechwycenia hasła – weryfikacja pod katem możliwości złamania hasła

11. Zdalne testy adresów publicznych

12. Badanie ankietowe

Badanie ankietowe pracowników działu IT oraz pracowników Zamawiającego z wiedzy o bezpieczeństwie sieci i procedurach IT stosowanych przez Zamawiającego. Grupa ankietowanych pracowników zostanie ustalona podczas Audytu.

13. Testy socjotechniczne

• kontakt bezpośredni – do 5 osób

• kontakt telefoniczny – do 10 osób

• kampanie phishingowe – możliwa dla całej organizacji

14. Wykonanie raportu zawierającego:

• opis wszystkich elementów, które zostały poddane audytowi

• podział podatności ze względu na ryzyko:

* 1. wysoki
	2. średni
	3. niski

• wskazanie zaleceń, rekomendacji, najlepszych praktyk – dla każdej znalezionej podatności

• wylistowanie wszystkich podatności ze względu na ryzyko:

* 1. wysoki
	2. średni
	3. niski

• określenie bezpieczeństwa informatycznego w organizacji poprzez wskazanie ilości i rodzaju

znalezionych podatności

15. Wsparcie poaudytowe

Udzielenie informacji na temat audytowanych elementów wynikających z raportu. Czas dla klienta na zapoznanie się z raportem i zadawanie pytań odnośnie raportu.

Ogólny opis przedsięwzięcia

1. Przedmiotem niniejszego zamówienia jest wykonanie diagnozy cyberbezpieczeństwa wraz z wykonaniem testów i raportu dotyczącego wszystkich elementów poddanych audytowi oraz wsparciem poaudytowym.

Pozostałe elementy zamówienia

2. Forma wynagrodzenia ryczałtowego (art. 632 KC) wymaga od Wykonawcy również wyceny ryzyka, bowiem Wykonawca nie będzie mógł żądać zmiany wynagrodzenia ryczałtowego dla zakresu dostaw objętych niniejszym zamówieniem.

3. Wykonawca jest odpowiedzialny za staranne zaznajomienie się z dokumentacją przetargową.

4. Wykonawca ma obowiązek na materiałach informacyjnych/szkoleniowych stosować oznakowanie zgodnie z aktualnymi zasadami informacji i promocji dla Programu Polska Cyfrowa w szczególności zgodnie z Kartą wizualizacji Programu Polska Cyfrowa na lata 2014-2020.

5. RODO: Dane osobowe Wykonawcy usługi, podwykonawców oraz dane zawarte w dokumentacji powykonawczej będą przechowywane przez cały okres trwałości projektu unijnego.

Część 2:

Usługa szkolenia pracowników Urzędu Miasta Puck z zakresu cyberbezpieczeństwa.

Ogólny opis przedsięwzięcia

1. Przedmiotem niniejszego zamówienia jest przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa dla pracowników Urzędu Miasta Puck.

2. Szkolenie zostanie przeprowadzone zgodnie z harmonogramem uzgodnionym z Zamawiającym.

3. Szkolenie odbędzie się w siedzibie Zamawiającego

4. Szkolenie zostanie przeprowadzone dla 57 pracowników Urzędu Miasta Puck.

5. Wszelkie materiały szkoleniowe powinny zawierać logotypy programu dostępne u Zamawiającego

Szkolenie powinno obejmować następujące zagadnienia:

1. Zakres i atrybuty bezpieczeństwa informacji.

2. Istotne obszary bezpieczeństwa z punktu widzenia pracowników Urzędu Miasta Puck z uwzględnieniem:

 bezpieczeństwa fizycznego (miejsca pracy),

 bezpieczeństwa organizacyjnego (personalnego),

 bezpieczeństwa informacyjnego (informacje, dane, zasoby).

3. Współczesne zagrożenia bezpieczeństwa informacji, ze szczególnym uwzględnieniem

cyberbezpieczeństwa oraz zagrożeń występujących podczas telepracy i pracy zdalnej.

4. Rodzaje ataków (m.in. spoofing, phishing, pharming, sniffing, ransomeware, malware) – przyczyny, źródła, cel i mechanizmy ataków.

5. Postępowanie w celu zapewnienia bezpieczeństwa informacji, w szczególności w ramach telepracy

i pracy zdalnej, omówienie zasad bezpieczeństwa informacji oraz najlepszych praktyk zabezpieczających:

 zasady bezpiecznego użytkowania sprzętu,

 procedura bezpiecznego logowania do aplikacji i systemów teleinformatycznych,

 bezpieczne przechowywanie haseł,

 odzyskiwanie hasła i dostępu do systemu operacyjnego,

 bezpieczne korzystanie z poczty elektronicznej,

 bezpieczne przechowywanie danych na laptopie i pendrivie,

 bezpieczne korzystanie z sieci Wi-Fi oraz zdalnego dostępu do firmowych zasobów,

 zasada „czystego biurka” i „czystego ekranu”,

 zasady bezpieczeństwa podczas wideokonferencji,

 bezpieczne korzystanie z Internetu, ze szczególnym uwzględnieniem serwisów

społecznościowych,

 metody ochrony przed atakami komputerowymi i socjotechnicznymi,

 stosowanie technik socjotechnicznych w informatyce – zdefiniowanie pojęcia przy użyciu

przykładów, z którymi pracownicy mogą spotkać się w codziennej pracy, przedstawienie

sposobów manipulacji mających na celu uzyskanie określonych korzyści, zwrócenie uwagi,

że nawet najmniejsza ilość informacji może przyczynić się do penetracji organizacji,

 przeciwdziałanie atakom socjotechnicznym (np. podszywanie się pod służby ochrony,

współpracownika lub firmę współpracującą, interesanta, pracownika biurowego na urlopie itp.;

profilowanie, zbieranie informacji o podmiocie ataku i wybieranie najlepszego czasu na atak),

 pakiet biurowy i niebezpieczne dokumenty (m.in. bezpieczna konfiguracja pakietu, złośliwe

makra, kradzież danych logowania i inne potencjalne ataki).

6. Przykłady incydentów bezpieczeństwa informacji.

Ostateczny program szkolenia zostanie ustalony z Zamawiającym.

Pozostałe elementy zamówienia

6. Forma wynagrodzenia ryczałtowego (art. 632 KC) wymaga od Wykonawcy również wyceny ryzyka, bowiem Wykonawca nie będzie mógł żądać zmiany wynagrodzenia ryczałtowego dla zakresu dostaw objętych niniejszym zamówieniem.

7. Wykonawca jest odpowiedzialny za staranne zaznajomienie się z dokumentacją przetargową.

8. RODO: Dane osobowe Wykonawcy usługi, podwykonawców oraz dane zawarte w dokumentacji powykonawczej będą przechowywane przez cały okres trwałości projektu unijnego.

**Wykonawca może opisać przedmiot zamówienia przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, jeżeli nie można opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób, a wskazaniu takiemu towarzyszyć będą wyrazy „lub równoważny”. Jeżeli Wykonawca opisze przedmiot zamówienia w sposób, o którym mowa wyżej, wówczas wskaże w opisie przedmiotu zamówienia także kryteria stosowane w celu oceny równoważności.**

|  |  |
| --- | --- |
| Nr postępowania: **RGKiM.271.12.2022.WJa** | ***Załącznik nr 8 do SWZ******składany na wezwanie Zamawiającego*** |

|  |  |
| --- | --- |
| **Zamawiający** | **Wykonawca** |
| **Gmina Miasta Puck**ul. 1 Maja 1384-100 Puck | ………………………………………………………………………………………………………………………………………………………………………………………*(pełna nazwa, adres)* |

**Wykaz wykonanych usług**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn.

**Usługi z zakresu cyberbezpieczeństwa dla Gminy Miasta Puck w ramach projektu grantowego „Cyfrowa Gmina”. W podziale na części:**

**1. Usługa wykonania diagnozy cyberbezpieczeństwa dla Urzędu Miasta Puck.**

**2.** **Usługa szkolenia pracowników Urzędu Miasta Puck z zakresu cyberbezpieczeństwa.**

prowadzonego przez **Gminę Miasta Puck** przedstawiam wykaz usług zrealizowanych w ciągu ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy, to w tym okresie, zgodnie z Rozdziałem VIII ust. 2 pkt 4 SWZ.

Ad. 1. Dla części nr 1 Usługa wykonania diagnozy cyberbezpieczeństwa dla Urzędu Miasta Puck.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L.p. | Zamawiający(nazwa i adres) | Krótki opis wykonanych usług (zakres, lokalizacja) | Wartość wykonanych usług(brutto) | Data zawarcia umowy oraz termin realizacji |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Ad. 2. Dla części nr 2 Usługa szkolenia pracowników Urzędu Miasta Puck z zakresu cyberbezpieczeństwa.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L.p. | Zamawiający(nazwa i adres) | Krótki opis wykonanych usług(zakres, lokalizacja) | Wartość wykonanych usług(brutto) | Data zawarcia umowy oraz termin realizacji |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

***Uwaga!***

*Do wykazu należy załączyć dowody potwierdzające, że usługi te zostały wykonane należycie i prawidłowo ukończone. Przy czym dowodami, o których mowa są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego usługi zostały wykonane, a jeżeli Wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – inne odpowiednie dokumenty.*

|  |  |
| --- | --- |
| **Miejscowość i data** | **Podpis Wykonawcy lub osoby uprawnionej do reprezentowania Wykonawcy*****Wymagany elektroniczny podpis kwalifikowany lub podpis zaufany lub podpis osobisty*** |
| ……………………………………… |  |

|  |  |
| --- | --- |
| Nr postępowania: **RGKiM.271.12.2022.WJa** | ***Załącznik nr 9 do SWZ******składany na wezwanie Zamawiającego*** |
| **Zamawiający** | **Wykonawca** |
| **Gmina Miasta Puck**ul. 1 Maja 1384-100 Puck | ………………………………………………………………………………………………………………………………………………………………………………………*(pełna nazwa, adres)* |

**Wykaz osób**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn.

**Usługi z zakresu cyberbezpieczeństwa dla Gminy Miasta Puck w ramach projektu grantowego „Cyfrowa Gmina”. W podziale na części:**

**1. Usługa wykonania diagnozy cyberbezpieczeństwa dla Urzędu Miasta Puck.**

prowadzonego przez **Gminę Miasta Puck** przedstawiam wykaz osób, które będą uczestniczyć przy realizacji niniejszego zamówienia, zgodnie z Rozdziałem VIII ust. 2 pkt 4 b SWZ.

|  |  |  |
| --- | --- | --- |
| **Nazwiska i imiona**osób, które będą pełnić poszczególne funkcje wraz z podstawą dysponowania | Wymagania Zamawiającego | Informacje na temat kwalifikacji zawodowych niezbędnych do wykonania zamówienia |
| Audytor (dane osobowe)…………………………………...…………………………………...*(podstawa dysponowania)* | Posiadanie uprawnień uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu. | …………………………………...*(nr uprawnień)* |

***Uwaga!*** *Do wykazu należy załączyć dowody potwierdzające, że osoby wyżej wymienione posiadają wymagane uprawnienia w postaci kopii wskazanych uprawnień (w przypadku podmiotów krajowych, dla podmiotów zagranicznych dokumenty równoważne).*

|  |  |
| --- | --- |
| **Miejscowość i data** | **Podpis Wykonawcy lub osoby uprawnionej do reprezentowania Wykonawcy*****Wymagany elektroniczny podpis kwalifikowany lub podpis zaufany lub podpis osobisty*** |
| ……………………………………… |  |

1. Zgodnie z treścią 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, zwanej dalej „ustawą”,* z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:

1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;

2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;

3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy. [↑](#footnote-ref-1)
2. Zgodnie z treścią 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, zwanej dalej „ustawą”,* z postępowania o udzielenie zamówienia publicznego lub konkursu prowadzonego na podstawie ustawy Pzp wyklucza się:

1) wykonawcę oraz uczestnika konkursu wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;

2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy;

3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 ustawy. [↑](#footnote-ref-2)