

Gołdap, dn.30.04.2025 r.

Znak postępowania OR.272.4.2025

SZACOWANIE WARTOŚCI ZAMÓWIENIA

I ZAMAWIAJĄCY

Powiat Gołdapski
ul. Krótka 1
19-500 Gołdap
NIP: 8471516948,
REGON: 519634600

II PRZEDMIOT ZAMÓWIENIA

1. Przedmiotem zamówienia jest:

- a) Opracowanie, aktualizacja i wdrożenie Systemów Zarządzania Bezpieczeństwem Informacji (SZBI) dla Starostwa Powiatowego w Gołdapi oraz 7 jednostek organizacyjnych Powiatu Gołdapskiego zakończone przeprowadzeniem powdrożeniowych szkoleń ze stosowania tych systemów dla pracowników i kadry zarządzającej,
- b) przeprowadzenie podstawowych szkoleń z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa dla pracowników oraz kadry zarządzającej jednostek organizacyjnych Powiatu Gołdapskiego,

w ramach projektu **„Podniesienie poziomu cyberbezpieczeństwa jednostek organizacyjnych Powiatu Gołdapskiego”**

III Opracowanie i wdrożenie Systemów Zarządzania Bezpieczeństwem Informacji (SZBI)

Wykonawca zobowiązany jest wytworzyć spójne, jednolite, adekwatne do faktycznych ryzyk, procesów i potrzeb Starostwa oraz Jednostek Podległych dokumentacje zgodne z wymaganiami norm rodziny ISO 2700 w zakresie bezpieczeństwa informacji (w szczególności zgodnego z wymaganiami aktualnej normy PN-EN ISO/IEC 27001) oraz rozporządzenia KRI.

1. Analiza stanu istniejącego i określenie wymagań:

- 1.1. realizacja audytów wstępnych mających na celu szczegółową analizę obecnych procesów, procedur operacyjnych oraz mechanizmów kontroli związanych z bezpieczeństwem informacji, w celu zidentyfikowania istniejących luk i obszarów wymagających usprawnienia, wywiad z pracownikami odpowiadającymi za bezpieczeństwo informacji, weryfikacja

zgodności dokumentacji oraz procedur związanych z bezpieczeństwem informacji pod kątem wymagań normy ISO 27001 oraz wymagań KRI i dyrektywy NIS2, analiza luk, opracowanie raportu uwzględniającego Starostwo oraz Jednostki Podległe (każda jednostka opisana odrębnie),

- 1.2. przeprowadzenie analiz ryzyka w ramach SZBI zakończonych raportem spełniające wymagania audytu o którym mowa w Rozporządzeniu Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

2. Opracowanie Dokumentacji SZBI oraz jej wdrożenie:

- 2.1. konstrukcja polityki bezpieczeństwa informacji na podstawie istniejącej dokumentacji SZBI, stworzenie kompletnego zestawu dokumentacji spełniającego wymagania normy PNISO/IEC 2700 oraz wymagania KRI, dyrektywy NIS2, dopasowanego do wymagań Starostwa oraz Jednostek Podległych. Dostosowanie dokumentacji oraz procesów ochrony danych osobowych do wymogów Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych,
- 2.2. rozwój i formalizacja procedur, instrukcji operacyjnych, wytycznych oraz innych dokumentów kluczowych dla wdrożenia i efektywnego funkcjonowania SZBI, uwzględniając przy tym specyfikę organizacyjną Starostwa oraz Jednostek Podległych oraz dopasowanie ich do wymagań wspólnie z Zamawiającym w celu osiągnięcia konsensusu co do finalnej formy i treści dokumentów,
- 2.3. opracowane polityki, procedury itd. muszą realnie odnosić się do procesów w Starostwie oraz w Jednostkach Podległych. Zamawiający oczekuje, że opracowane dokumenty będą napisane zwięźle, językiem zrozumiałym dla osób nie posiadających wysokich kompetencji z zakresu bezpieczeństwa informacji.
- 2.4. Wsparcie przy wdrożeniu dokumentacji w zakresie implementacji najlepszych praktyk dotyczących wdrożenia procedur i polityk określonych w dokumentacji SZBI,
- 2.5. Wykonawca powinien zapewnić minimum 6 godzin zegarowych konsultacji dla każdej jednostki objętej usługą.

3. Oczekiwany efekt końcowy wdrożenia SZBI:

Finalizacja usługi zapewni Starostwu oraz Jednostkom Podległym, kompleksową, spójną oraz w pełni funkcjonalną dokumentację SZBI, która stanie się solidnym fundamentem dla efektywnego zarządzania bezpieczeństwem informacji. Dzięki temu, organizacja uzyska dogłębne zrozumienie metod zarządzania ryzykiem, ochrony informacji oraz adaptacji do zmieniających się zagrożeń, co w konsekwencji umożliwi ciągłe doskonalenie systemu bezpieczeństwa informacji.

Opracowana dokumentacja SZBI stanie się kluczowym elementem w strukturze zarządzania organizacją, zapewniając nie tylko zgodność z międzynarodowymi normami i najlepszymi praktykami, ale również dopasowanie do specyficznych wymogów i oczekiwań Zamawiającego.

Dokumentacja ta będzie również służyć jako instrukcja operacyjna dla wszystkich pracowników i zainteresowanych stron, ułatwiając zrozumienie ich ról i odpowiedzialności w kontekście bezpieczeństwa informacji. W rezultacie, wszyscy uczestnicy procesu będą mieli jasne wytyczne dotyczące sposobu postępowania, co znacznie zwiększy ogólną świadomość bezpieczeństwa w organizacji oraz efektywność wdrażanych środków ochronnych. Takie podejście zapewni organizacji nie tylko obronę przed potencjalnymi zagrożeniami, ale także pozytywnie wpłynie na reputację wśród klientów, partnerów biznesowych oraz innych interesariuszy, budując zaufanie poprzez demonstrację zaangażowania w ochronę poufnych informacji i danych osobowych. Finalnie, kompletna i zaktualizowana dokumentacja SZBI będzie stanowić nieoceniony zasób w procesie ciągłego monitorowania, przeglądania i ulepszania procesów bezpieczeństwa, umożliwiając organizacji dynamiczne reagowanie na nowe wyzwania i zapewniając stabilność operacyjną w zmieniającym się środowisku.

IV Szkolenia pracowników:

1. Szkolenie ma na celu poszerzenie wiedzy pracowników na temat bezpiecznego korzystania z cyberprzestrzeni w miejscu pracy i poza nim co najmniej w zakresie:
 - a) czym jest cyberbezpieczeństwo?
 - b) omówienie poprawnych zasad związanych z cyberbezpieczeństwem w Urzędzie,
 - c) jak definiować i charakteryzować najważniejsze techniki cyberataków,
 - d) jak rozpoznawać i zapobiegać zagrożeniom związanym z cyberprzestrzenią,
 - e) jak podejmować odpowiednia działania w przypadku cyberataku,
 - f) jak stosować odpowiednie zabezpieczenia utrudniające przeprowadzenie cyberataku,
 - g) jak rozpoznawać socjotechniki wykorzystywane przez cyberprzestępców.
 - h) szczegółowe omówienie zagrożeń w sieci takich jak phishing, ransomware, malware, socjotechnika, atak telefoniczny, spoofing, atak odwrócony - zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa, fałszywe wiadomości

mailowych, SMS wraz z przykładami i wskazaniem sposobów przeciwdziałania oraz zabezpieczania się przed powyższymi zagrożeniami,

- i) metody nieautoryzowanego pozyskania danych wraz z przykładami
 - j) bezpieczne przetwarzanie danych: szyfrowanie, przechowywanie, udostępnianie, komunikacja
 - k) bezpieczne hasła, menedżer haseł, autoryzacja dwuetapowa, klucze sprzętowe
 - l) metody obrony oraz przeciwdziałania (w tym: przed wyłudzeniem danych osobowych za pomocą metod socjotechnicznych, programowaniem mogącym zablokować dostęp do urządzeń urzędu, szkodliwymi programami mogącymi pozyskać dane firmowe lub osobiste
 - m) bezpieczne korzystanie z mediów społecznościowych
 - n) bezpieczne korzystanie ze smartfonów
 - o) wskazanie miejsc organizacji oraz informacji, które należy chronić, by zniwelować ryzyko narażenia firmy na straty finansowe.
 - p) stosowania wdrożonych polityk SZBI i procedur
2. Szkolenie (miejsce, ilość grup szkoleniowych) należy przeprowadzić w sposób uzgodniony z Zamawiającym.
 3. Szkolenie należy przeprowadzić z uwzględnieniem faktu, że uczestnicy szkolenia mogą nie posiadać wiedzy informatycznej i technicznej,
 4. Czas trwania szkolenia dla pojedynczej grupy szkoleniowej – co najmniej 4 godziny zegarowe.
 5. Wykonawca w ramach wykonania usługi przygotowuje harmonogram szkolenia oraz program szkolenia i dostarczy je w terminie nie później niż 10 dni roboczych przed dniem rozpoczęcia szkolenia do akceptacji Zamawiającego.
 6. Harmonogram powinien obejmować informacje dotyczące tematyki i czasu szkolenia
 7. Wykonawca przygotowuje i zapewni materiały szkoleniowe dla każdego uczestnika, pozwalające na samodzielną edukację z zakresu tematyki szkolenia.
 8. Zamawiający dopuszcza dostarczenie każdemu użytkownikowi kompletu materiałów w formie elektronicznej, np. dokumenty w standardzie PDF
 9. Wykonawca dostarczy materiały szkoleniowe uczestnikom szkolenia najpóźniej w dniu rozpoczęcia szkolenia
 10. Wykonawca przygotowuje Zamawiającemu materiały ze szkolenia, które to będzie mógł wykorzystać do przeszkolenia osób nieobecnych lub nowo przyjętych.
 11. Wszelkie koszty opracowania materiałów szkoleniowych ponosi Wykonawca
 12. Wykonawca nie jest zobowiązany do zapewnienia uczestnikom wyżywienia
 13. Wykonawca umożliwi uczestnikom skorzystać z konsultacji po ukończeniu szkolenia

14. Szkolenie musi być certyfikowane. Wykonawca w ramach wynagrodzenia zapewni uczestnikom szkolenia imienne certyfikaty potwierdzające ukończenie szkolenia i jego zakres.

V Szkolenia kadry zarządzającej:

Szkolenie ma na celu poszerzenie wiedzy kadry zarządzającej na temat bezpiecznego korzystania z cyberprzestrzeni w miejscu pracy i poza nim co najmniej w zakresie tożsamym z szkoleniami pracowników.

Szkolenie musi obejmować tematy związane ze stosowaniem wdrożonych polityk SZBI i procedur, przez kadrę zarządzającą oraz obowiązki wynikające z aktualnych przepisów prawa.

VI Informacje dotyczące szacowanej liczby pracowników, w poszczególnych jednostkach:

- a) Starostwo Powiatowe w Gołdapi - 46,
- b) Powiatowy Urząd Pracy w Gołdapi - 23,
- c) Zarząd Dróg Powiatowych w Gołdapi - 5,
- d) Powiatowe Centrum Pomocy Rodzinie w Gołdapi - 10,
- e) Poradnia Psychologiczno-Pedagogiczna w Gołdapi - 12
- f) Liceum Ogólnokształcące im. Jana Pawła II w Gołdapi - 28
- g) Zespół Szkół Zawodowych w Gołdapi - 49
- h) Zespół Placówek Edukacyjno-Wychowawczych w Gołdapi - 49

VII Płatność

- a) Wynagrodzenie nastąpi na podstawie faktury wystawionej po podpisaniu bez zastrzeżeń protokołu odbioru.
- b) Wynagrodzenie będzie płatne w terminie 14 dni od daty dostarczenia Zamawiającemu prawidłowo wystawionej faktury VAT, przelewem na rachunek Wykonawcy podany na fakturze. W przypadku opóźnienia w zapłacie Wynagrodzenia Zamawiający zobowiązany będzie do zapłaty odsetek ustawowych za opóźnienie na rzecz Wykonawcy.
- c) [Jeśli dotyczy] Wykonawca oświadcza, że jest czynnym podatnikiem VAT oraz potwierdza, że nazwa firmy, adres prowadzenia działalności, NIP oraz nr rachunku bankowego podany na fakturze są zgodne z wykazem podatników VAT prowadzonym przez Szefa Krajowej Administracji Skarbowej oraz potwierdza możliwość dokonywania płatności przez Zamawiającego metodą split payment.

VIII TERMIN REALIZACJI: do 150 dni od dnia podpisania umowy

IX KOD CPV

79212000-3 Usługi audytu

79417000-0 Usługi doradcze w zakresie bezpieczeństwa

80511000-9: Usługi szkolenia personelu

7963200-3: Szkolenie pracowników

X TRYB UDZIELENIA ZAMÓWIENIA

1. Procedura prowadzona w trybie zapytania ofertowego zgodnie Wytycznymi w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2021-2027,
2. Zamawiający nie dopuszcza możliwości składania ofert wariantowych.
3. Zamawiający nie przewiduje udzielenia zamówień uzupełniających

XI WARUNKI UDZIAŁU W POSTĘPOWANIU

1. O zamówienie mogą ubiegać się wykonawcy, którzy:
 - a) posiadają odpowiednie zaplecze techniczne i osobowe gwarantujące prawidłową realizację usługi.
 - b) w zakresie osób zdolnych do wykonania zamówienia, w zespole opracowującym dokumentację SZBI musi być przynajmniej 1 osoba posiadająca certyfikat Audytora wiodącego ISO/IEC 27001 w wersji 2007 albo 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).
 - c) posiadają wpis do Rejestru Instytucji Szkoleniowych (RIS)
 - d) wykażą, że ciągu ostatnich 3 lat, a jeśli okres prowadzenia działalności jest krótszy, to w okresie prowadzenia działalności, rzetelnie wykonali co najmniej 1 szkolenie z zakresu cyberbezpieczeństwa i przeszkolili co najmniej 50 osób (Załącznik nr 2- Wykaz usług).
2. Zamawiający oceni spełnienie warunku udziału w postępowaniu na podstawie złożonych przez Wykonawcę oświadczeń i dokumentów. Do wykazu załączyć należy dowody potwierdzające, że usługa wykonana została w sposób należyty, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane w sposób należyty.

XII MIEJSCE, TERMIN ORAZ SPOSÓB SKŁADANIA OFERT (formularza szacowania)

1. Oferta ma być sporządzona w języku polskim pod rygorem nieważności.
2. Ofertę podpisuje osoba uprawniona do składania oświadczeń woli w imieniu Wykonawcy. Upoważnienie do podpisania oferty powinno być dołączone do oferty, o ile nie wynika z innych dokumentów dołączonych do oferty.
3. Do oferty należy dołączyć:

- a) wykaz usług wraz z dowodami potwierdzającymi, że te usługi zostały wykonane lub są wykonywane należycie,
 - b) upoważnienie do podpisania oferty lub dokumenty, z których wynika umocowanie do podpisania oferty przez osobę podpisującą
4. Ofertę należy składać na formularzu ofertowym wraz z wymaganymi załącznikami na adres informatyk@powiatgoldap.pl
 5. Termin składania ofert: do dnia 05.05.2025 r. do godz. 13:00
 6. Osoba do kontaktów: Łukasz Dębowski, email: informatyk@powiatgoldap.pl
 7. Oferent winien posiadać prawo do występowania w obrocie prawnym i prowadzić działalność gospodarczą, której przedmiot jest zgodny z treścią zamówienia. Dokumenty składające się na ofertę mogą być złożone w oryginale lub kopii potwierdzonej za zgodność z oryginałem przez Wykonawcę.
 8. Oferty złożone w inny sposób bądź po terminie podanym w niniejszym punkcie będą podlegały odrzuceniu.
 9. Wykonawca może złożyć tylko jedną ofertę.
 10. Cena oferty to cena ofertowa brutto wymieniona w formularzu ofertowym. W cenie oferty należy zawrzeć wszystkie koszty związane z realizacją przedmiotu zamówienia. Prawidłowe ustalenie podatku VAT należy do obowiązków Wykonawcy.
 11. Wszystkie ceny muszą być wyrażone w złotych polskich z dokładnością do dwóch miejsc po przecinku. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone wyłącznie w złotych polskich.
 12. Wykonawca jest zobowiązany do załączenia dokumentów potwierdzających uprawnienia osób podpisujących ofertę do reprezentowania Wykonawcy, o ile nie wynikają z przepisów prawa lub innych dokumentów rejestrowych, aktualnych na dzień podpisania oferty. W przypadku braku ww. dokumentu Zamawiający wezwie Wykonawcę jednokrotnie do jego uzupełnienia pod rygorem odrzucenia oferty.

XIII POZOSTAŁE

1. Zadanie przewidziane do realizacji jest przy współudziale środków zewnętrznych - dofinansowania z „Cyberbezpiecznego Samorządu”.
2. Niniejsze postępowanie prowadzone jest na zasadach opartych na wewnętrznych uregulowaniach Zamawiającego. Postępowanie prowadzone jest zgodnie z zasadą konkurencyjności i nie podlega przepisom Prawo zamówień publicznych.
3. Do prowadzonego postępowania nie przysługują Wykonawcom żadne środki ochrony prawnej określone w przepisach ustawy Prawo zamówień publicznych tj. odwołanie, skarga.
4. Zamawiający zastrzega sobie prawo do zmiany zapytania ofertowego przed upływem terminu do składania ofert. Wszelkie zmiany treści zapytania ofertowego oraz wyjaśnienia udzielone na zapytania Wykonawcy stają się integralną częścią zapytania ofertowego i są wiążące dla Wykonawców.

5. Zamawiający zastrzega sobie prawo do unieważnienia niniejszego postępowania w każdym czasie bez podania uzasadnienia, w tym także pozostawienia postępowania bez wyboru oferty.
6. Wykonawcy, których oferty nie zostaną wybrane nie mogą zgłaszać żadnych roszczeń względem Zamawiającego z tytułu otrzymania zapytania ofertowego oraz przygotowania i złożenia oferty na to zapytanie.
7. Zamawiający zastrzega sobie prawo (możliwość) do zamieszczenia na stronie internetowej prowadzonego postępowania informacji o: złożonych ofertach, wynikach postępowania (udzieleniu zamówienia).
8. Wykonawca, którego oferta zostanie wybrana zostanie powiadomiony pisemnie lub telefonicznie o wyborze jego oferty oraz o terminie i miejscu podpisania (zawarcia) umowy (zlecenia). Zamawiający nie określa (nie przewiduje) warunków istotnych zmian umowy zawartej w wyniku przeprowadzonego postępowania o udzielenie zamówienia.
9. Jeżeli Wykonawca, którego oferta została wybrana uchyla się od podpisania umowy, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert.

XIV Zapewnienie dostępności osobom ze szczególnymi potrzebami

W związku z obowiązkiem określenia przez Zamawiającego warunków służących zapewnieniu dostępności osobom ze szczególnymi potrzebami w zakresie tych zadań publicznych lub zamówień publicznych, wynikającym z art. 4 ust. 3 ustawy o Zapewnieniu dostępności osobom ze szczególnymi potrzebami (tj. Dz. U. 2022 poz. 2240 z późn. zm.), Zamawiający informuje, że w prowadzonym postępowaniu w żadnym z trzech wskazanych zakresów tj.: w zakresie dostępności architektonicznej, w zakresie dostępności cyfrowej, w zakresie dostępności informacyjno- komunikacyjnej, nie występują przesłanki do określenia wyżej wspomnianych warunków z