Szacowanie wartości zamówienia

SIWZ - Specyfikacja Istotnych Warunków Zamówienia / OPZ – Opisz przedmiotu zamówienia

1. Gmina Istebna, Istebna 1000, 43-470 Istebna, NIP: 5482676134, zaprasza do składania ofert cenowych w ramach **szacowanie wartości zamówienia** na: **Opracowanie i wdrożenie kompleksowego systemu zarządzania bezpieczeństwem informacji, szkolenia i pozostałe usługi cyberbezpieczeństwa dla Gminy Istebna w ramach projektu pn. „Wzmocnienie poziomu cyberbezpieczeństwa w gminie Istebna" realizowanego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23".**

   Postępowanie prowadzone jest w celu oszacowania wartości zamówienia.

2. Przedmiotem niniejszego zamówienia jest:

   Opracowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (nazywanego dalej SZBI) w oparciu o norm rodziny ISO 27000 w zakresie bezpieczeństwa informacji oraz Narodowy Standard Cyberbezpieczeństwa NSC 200 wer. 2.1 Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych (w szczególności PN-EN ISO/IEC 2701), oraz Systemu Zarządzania Ciągłością Działania w oparciu o normą PN-EN ISO 22301.

   Wykonawca zobowiązany jest wytworzyć spójne, jednolite, adekwatne do faktycznych ryzyk, procesów i potrzeb Urzędu dokumentacje SZBI oraz planu ciągłości działania zgodne z wymaganiami powołanych wyżej norm / standardów.

   Cel główny projektu:

Zwiększenie poziomu dostępności i efektywności bezpiecznych usług świadczonych przez Urząd w postaci elektronicznej na rzecz obywateli i podmiotów gospodarki narodowej oraz administracji publicznej.

Cele szczegółowe projektu:

1. Opracowanie/przygotowanie dokumentacji bezpieczeństwa informacji w jednostce publicznej.

2. Zwiększenie poziomu bezpieczeństwa danych.

3. Zwiększenie świadomości i kompetencji pracowników w zakresie bezpieczeństwa informacji.

4. Wsparcie zarządzania incydentami bezpieczeństwa, zapewnienie kontrolowanej analizy zagrożeń.

Systemu Zarządzania Bezpieczeństwem Informacji musi być zgodny z następującymi aktami prawnymi:

- ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (w zakresie dotyczącym bezpieczeństwa informacji),
- rozporządzenie 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,
- i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (w zakresie dotyczącym bezpieczeństwa informacji),
- rozporządzenie 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 ochronie danych),

- ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,

- Dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (tzw. Dyrektywa NIS 2).

W szczególności wymagany zakres prac obejmuje:

2.1. Audyt wstępny Urzędu obejmujący:

2.1.1. sprawdzenie i zrozumienie środowiska, obejmujący aktualną strukturę organizacyjną i realizowane procesy oraz wymagania prawne funkcjonowania,

2.1.2. przegląd aktualnej dokumentacji bezpieczeństwa informacji, w tym polityk, procedur, instrukcji, regulaminów, wytycznych,

2.1.3. wywiady z przedstawicielami Urzędu,

2.1.4. obserwacje audytora, dotyczące bezpieczeństwa fizycznego i środowiskowego,

2.1.5. obserwacje audytora, dotyczące bezpieczeństwa serwerowni,

2.1.6. obserwacje audytora dotyczące bezpieczeństwa kluczowych systemów teleinformatycznych.

2.1.7. przeprowadzenie przy udziale przedstawicieli Zamawiającego inwentaryzację i analizę aktywów - zasobów informacyjnych oraz środków służących do gromadzenia i przetwarzania informacji, oraz pozostałych procesów celem wypracowania Rejestru Przetwarzania zgodnego z RODO.

2.1.8. audyt będzie uwzględniał co najmniej:

• wymagania KRI/UoKSC
• Audyt Techniczny – wymagań zawartych w załączniku A normy ISO/IEC 27001
• Audyt Systemowy – wymagań normy zawartych normie ISO/IEC 27001
• Audyt Ciągłości Działania – wymagań normy zawartych normie ISO/IEC 22301

oraz obszary określone w normie PN-EN ISO/IEC 27001:

- ✓ kontekst organizacji,
- ✓ polityki bezpieczeństwa informacji i inne dokumenty dotyczące bezpieczeństwa informacji,
- ✓ organizacja bezpieczeństwa informacji,
- ✓ postepowanie z ryzykiem w bezpieczeństwie informacji,
- ✓ bezpieczeństwo zasobów ludzkich,
- ✓ zarządzanie aktywami,
- ✓ kontrola dostępu,
- ✓ kryptografia,
- ✓ bezpieczeństwo fizyczne i środowiskowe,

- ✓ bezpieczna eksploatacja,
- ✓ bezpieczeństwo komunikacji,
- ✓ pozyskiwanie, rozwój i utrzymanie systemów,
- ✓ relacje z dostawcami,
- ✓ zarządzanie incydentami związanymi z bezpieczeństwem informacji,
- ✓ zarządzanie ciągłością działania,
- ✓ zgodność

Audyt powinien zawierać także wskazania podatności systemów informatycznych: wskazanie podatności, wagi podatności, opis podatności, informacje dotyczące podatności w tym źródła zewnętrzne, rekomendacje co do sposobu postępowania.

2.1.9. raport z przeprowadzonego audytu bezpieczeństwa, przygotowany i przekazany Zamawiającemu w formie papierowej i elektronicznej będzie zawierał co najmniej:

- ✓ podsumowanie zarządcze,
- ✓ obszary sprawdzenia,
- ✓ metoda prowadzenia audytu,
- ✓ ocenę spełnienia wymagań,
- ✓ wydanie rekomendacji/zaleceń w przypadku stwierdzonych niezgodności i braków, które będą stanowiły podstawę do aktualizacji, dostosowania lub przygotowania dokumentacji SZBI

2.1.10. Minimalny czas trwania audytu uzależniony jest od realnych potrzeb czasowych związanych z ocena stanu faktycznego – czynności wykonywane na miejscu u Zamawiającego.

Zamawiający zastrzega sobie prawo do uwag do zawartości raportu z przeprowadzonego audytu bezpieczeństwa zgłaszanych w procedurze odbioru. Warunkiem odbioru raportu z przeprowadzonego audytu bezpieczeństwa jest jego akceptacja przez Zamawiającego. Potwierdzeniem wykonania raportu będzie, podpisany z wynikiem pozytywnym przez Strony, Protokół odbioru raportu z przeprowadzonego audytu bezpieczeństwa.

2.2. Przeprowadzenie przy udziale przedstawicieli Zamawiającego i udokumentowanie analizy ryzyka, w tym opracowanie i wdrożenie metodyki szacowania ryzyka zgodnie z wymaganiami normy ISO27005:2022,

2.2.1. Identyfikacja aktywów

2.2.2. Identyfikacja i ocena podatności, które mogą być wykorzystane przez zagrożenia dla aktywów

2.2.3. Identyfikacja i ocena skutków utraty poufności, integralności i dostępności w odniesieniu do aktywów

2.2.4. Ocena ryzyka

2.2.5. **Opracowanie narzędzia pliku EXCEL lub innego do automatyzacji analizy ryzyka na podstawie przyjętej metodologii zgodnej z normą w połączenie z planem ciągłości działania (jedno narzędzie). Plika musi być przejrzysty do udostępnienia konkretnych zakładek dla kierowników komórek organizacyjnych celem oszacowania ryzyka w danej komórce. Plik musi uwzględniać ryzyka RODO, Ustawy o Cuber bezpieczeństwie oraz norm ISO (dostarczone narzędzie i prawa autorskie do jego wykorzystywania zamiany / dostawania przechodzi na własność Gminy).**

2.2.6. Wskazanie obszarów wymagających dostosowania i/lub doskonalenia adekwatnie do przeprowadzonej analizy ryzyka oraz wymagane do wdrożenia zabezpieczenia.

2.3. Opracowanie kompletnej dokumentacji SZBI (polityk, planów, procedur, instrukcji, metodologii zarządzania ryzykiem itd.) oraz plan ciągłości działania w zakresie systemów informatycznych.

2.3.1. Opracowane polityki, procedury itd. muszą realnie odnosić się do procesów w Urzędzie. Zamawiający oczekuje, że opracowane dokumenty będą napisane zwięźle, językiem zrozumiałym dla osób nieposiadających wysokiego przygotowania z zakresu bezpieczeństwa informacji. Zamawiający oczekuje, że zostaną zinwentaryzowane wszystkie procesy przetwarzania i opracowany pełny rejestr czynności przetwarzania oraz pełły rejestr kategorii czynności przetwarzania według RODO.

2.3.2. Dokumentacja SZBI musi uwzględniać:

a) polityka bezpieczeństwa informacji
b) organizacja bezpieczeństwa informacji
c) bezpieczeństwo zasobów ludzkich
d) zarządzanie aktywami
e) przekazywanie nośników kontrola dostępu
f) kryptografia
g) bezpieczeństwo fizyczne i środowiskowe
h) bezpieczna eksploatacja
i) bezpieczeństwo komunikacji
j) pozyskiwanie, rozwój i utrzymanie systemów
k) relacje z dostawcami
l) zarządzanie incydentami związanymi z bezpieczeństwem informacji (w tym cyberbezpieczeństwa)

m) bezpieczeństwo informacji w zarządzaniu ciągłością działania

Dokumentacja SZBI powinien składać się z co najmniej następujących dokumentów:

1) Polityka Bezpieczeństwa Informacji,

2) Polityka Bezpieczeństwa Danych Osobowych,

3) Polityka bezpieczeństwa systemów teleinformatycznych (odniesienie do wszystkich posiadanych systemów u Zamawiającego z uwzględnieniem zabezpieczeń w każdym z systemów),

4) Regulamin Użytkownika Systemów Teleinformatycznych,

5) Procedura zarządzania incydentami bezpieczeństwa teleinformatycznego – cyberbezpieczeństwa

6) Analizy ryzyka,

7) Regulamin Bezpieczeństwa użytkowania komputerów przenośnych oraz wykonywania pracy zdalnej,

8) Regulamin korzystania ze służbowej poczty elektronicznej,

9) Plan ciągłości działania zgodny z PN-EN-ISO-22301_2020 (dotyczący każdego posiadanego systemu informatycznego oraz ogólnie całej infrastruktury sprzętowej (serwery, przełączniki, itp.):

- RPO (Recovery Point Objective): Określa, ile danych organizacja może utracić, wyrażając to w czasie wstecz, do którego dane muszą zostać odzyskane.
- RTO (Recovery Time Objective): Czas, w jakim systemy muszą być przywrócone po awarii, aby zminimalizować wpływ na działalność.
- MTD (Maximum Tolerable Downtime): Maksymalny dopuszczalny czas przestoju krytycznego procesu lub systemu bez powodowania trwałych szkód.
- Identyfikacja zasobów krytycznych: Lista kluczowych procesów, systemów i zasobów, które muszą być chronione.
- Procedury awaryjne: Szczegółowe instrukcje dotyczące działań w przypadku awarii lub zakłóceń.

- Komunikacja kryzysowa: Plan komunikacji z pracownikami, klientami i partnerami podczas awarii.
- Ocena ryzyka i BIA (Business Impact Analysis): Identyfikacja ryzyk i ich wpływu na działalność organizacji oraz krytycznych procesów wymagających ochrony.),

10) Procedura oceny skutków przetwarzania dla ochrony danych (DPIA),

11) Rejestr czynności przetwarzania, Rejestr kategorii czynności przetwarzania,

12) Deklaracja stosowania zgodnie z aktualną normą.

w/w dokumenty muszą zawierać procedur:

• Procedura nadzoru nad dokumentami

• Procedura działań korekcyjnych, korygujących i zapobiegawczych

• Procedura audytu wewnętrznego

• Procedura nadzoru nad zapisami

• Procedura przeglądu zarządzania

• Procedura zarządzania incydentami

• Procedura bezpieczeństwa wewnętrznego organizacji

• Procedura ewakuacji personelu i sprzętu z obiektów

• Procedura klasyfikacji informacji wewnętrznych i zewnętrznych

• Procedura oceny ryzyk generowanych przez strony zewnętrzne (klientów, dostawców, kooperantów, innych)

• Procedura postępowania w przypadku odejścia pracownika z firmy

• Procedura bezpieczeństwa infrastruktury teleinformatycznej (sieć, serwerownie, urządzenia łączności, inne elementy)

• Procedura bezpieczeństwa fizycznego

• Procedura nadzór nad przyrządami pomiarowymi i zapewnienia spójności pomiarowej

• Procedura wykorzystywania sprzętu służbowego co celów przydatnych;

• Procedura wykorzystywania sprzętu prywatnego do celów służbowych;

• Inne niezbędne u klienta z punktu widzenia systemu bezpieczeństwa informacji (po ocenie potrzeb)

• Dokumenty ustalające status systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami normy.

• Opracowanie formularzy i rejestrów będących integralną częścią w/w dokumentów w formie i treści odpowiedniej do potrzeb i woli klienta (zawartość merytoryczna oraz forma).

• Mapa procesów objętych SZBI, schemat procesów należy przygotować w notacji BPMN

• Deklaracja stosowania dla systemu bezpieczeństwa informacji wraz z przyporządkowanie aktualnie używanych w organizacji rozwiązań do wymagań normy.

• Plan ciągłości działania musi uwzględniać wszystkie zasoby u Zamawiającego jak również wszystkie procesy przetwarzania. Wykonawca musi wspólnie z Zamawiającym ustalić czasy RPO (Recovery Point Objective), RTO (Recovery Time Objective), MTD (Maximum Tolerable Downtime), BIA (Business Impact Analysis) jak również krytyczności danego zasobu i danego procesu. Wykonawca musi opracować plik EXCEL lub inny który następnie Zamawiający będzie mógł samodzielnie dowolnie dopasowywać do swoich potrzeb automatyzujący powiązania zasobów, procesów, krytyczności oraz musi być powiązany z analizą ryzyka zgodnie z przyjętą metodologią (jedno narzędzie). Czasy muszą obnosić się do zasobu np. klastra HA lub klastra replikacji który musi zawierać składowe klastra np. serwery, macierze itp. z określonymi również czasami i krytycznością. Plik i prawa autorskie opracowanego narzędzia przechodzą na Zamawiającego. Przejrzystość i zakres funkcjonalności przygotowanego narzędzia musi zostać pozytywnie zaakceptowany przez Zamawiającego celem dokonania odbioru. Zamawiający nie dopuszcza rozwiązania zamkniętego bez możliwości jego samodzielnej późniejszej modyfikacji oraz rozwiązania w chmurze.

2.3.3. Wykonawca w ramach dokumentów SZBI zaktualizuje lub opracuje dokument SZBI związany z zarządzaniem ryzykiem bezpieczeństwa informacji z uwzględnieniem punktu 2.2.

2.3.4. Wykonawca w ramach dokumentów SZBI przygotuje listę środków technicznych dla zapewnienia bezpieczeństwa informacji z uwzględnieniem środków wykorzystywanych przez Zamawiającego.

2.3.5. Wykonawca realizując SZBI uwzględni zmieniającą się infrastrukturę teleinformatyczną Zamawiającego. Zamawiający planuje w okresie świadczenia usługi przez Wykonawcę rozbudowę infrastruktury teleinformatycznej.

2.3.6. Wykonawca przygotuje harmonogram dostosowywania opracowywania poszczególnych dokumentów SZBI.

2.3.7. Harmonogram realizacji zadań musi uwzględniać przekazywanie przez Wykonawcę poszczególnych dokumentów etapami, w sposób pozwalający na weryfikację dokumentów przez Zamawiającego.

2.3.8. Zamawiający zastrzega sobie prawo do wniesienia uwag do treści dokumentacji SZBI, zgłaszanych w trakcie procedury odbiorowej.

2.3.9. Potwierdzeniem wykonania dokumentacji SZBI będzie podpisany z wynikiem pozytywnym przez Strony, Protokół odbioru dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

Jednocześnie Zamawiający zastrzega, że wszelkie błędy w przygotowanej dokumentacji świadczące o tym, że dokumentacja została przeniesiona z innej organizacji będą podstawą do odrzucenia dokumentów do poprawki, bez ich dalszej analizy ze strony Zamawiającego.

2.4. Przeprowadzenie szkoleń z zakresu zarządzania bezpieczeństwem informacji, budujące świadomość cyberzagrożeń i sposobów ochrony przed nimi w odniesieniu do całości SZBI stacjonarnie w siedzibie Zamawiającego dla:

2.4.1. wyższego kierownictwa – kierowników komórek organizacyjnych – co najmniej 2x4 godziny (2 szkolenie w różnych terminach ustalonych z Zamawiającym),

2.5.4. dla min. 75% pracowników (z wyłączeniem osób uczestniczących w wcześniej wymienianych szkoleniach) – co najmniej 2 x 6 godziny (2 szkolenie w różnych terminach ustalonych z Zamawiającym).

Łącznie 4 szkoleń 4 lub 6 godzinnych (jedna godzina to 45 minut zajęć).

2.5. Przeprowadzenie przy udziale Zamawiającego pełnego audytu końcowego po zakończeniu projektu Cyberbezpieczny Samorząd oraz ponowne wypełnienie Ankietę Dojrzałości

Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego zgodnie z zasadami projektu Cyberbezpieczny Samorząd – zakres i zasady audytu adekwatny jak w punkcie 2.1.

2.6. Audyt zgodności z KRI/UoKSC za rok 2025 – przedstawiony Zamawiającemu do końca września 2025 roku.

2.7. TESTY SOCJOTECHNICZNE DLA PRACOWNIKÓW

2.7.1. Zamawiający wymaga wykonania dwóch testów socjotecznicznych dla pracowników, każdy trwający od 1 do 3 dni kolejno po sobie następujących.

2.7.2. Termin realizacji zamówienia - test pierwszy w ciągu 3 miesięcy od dnia zawarcia umowy. Test drugi – do 30 października 2025, nie wcześniej niż po 12 miesiącach od zawarcia umowy, w terminie uzgodnionym z Zamawiającym.

2.7.3. Minimalny zakres testów socjotechnicznych:

- Kontakt mailowy z próbami pozyskania danych logowania (phishing, spear phishing),
- Kontakt mailowy z próbami aktywowania złośliwych linków,
- Kontakt mailowy z próbami nakłonienia do otwarcia wskazanego dokumentu,

2.7.4. Zamawiający wymaga wykonania testów socjotechnicznych dla min. 50% pracowników zatrudnionych w każdej jednostce. Wykaz osób zatrudnionych w poszczególnych jednostkach wraz z niezbędnymi danymi Zamawiający przekaże Wykonawcy po zawarciu umowy.

2.7.5. Zamawiający wymaga, aby wszystkie prace były prowadzone w sposób kontrolowany, gwarantujący poufność danych oraz bezpieczeństwo środowiska pracy. W przypadku udanych prób pozyskania poufnych danych (np. danych uwierzytelniających) osoba wyznaczona do kontaktu po stronie Zamawiającego musi być natychmiast informowana o zaistniałej sytuacji.

2.7.6. Potwierdzeniem wykonania każdego z testu (odrębnie 1 oraz 2) będzie opracowany raport z przeprowadzonych testów, prezentujący m.in. wykaz podjętych działań, w tym opis prób udanych oraz rekomendowane środki zaradcze, które pozwolą uniknąć podobnych sytuacji w przyszłości. Raport winien być sporządzony i przedłożony Zamawiającemu wraz z protokołem zdawczo-odbiorczym wykonania usługi po zakończeniu testów, nie później niż w ciągu 30 dni od zakończenia testu.

2.8. **Szkolenia specjalistyczne dla kadry IT z zakresu bezpieczeństwa sieci - systemów. Microsoft Unlimited - możliwość udziału w nielimitowanej ilości autoryzowanych szkoleń Microsoft na 12 miesięcy od daty zakupu. Szkolenia odbywają się w Wirtualnej klasie, na żywo, z certyfikowanym trenerem Microsoft. Abonament Microsoft Unlimited umożliwia korzystanie bez ograniczeń z pełnego wachlarza szkoleń online w terminach gwarantowanych minimum 7 szkoleń.**

Dodatkowo Wykonawca zapewnia 2 vouchery na egzaminy Microsoft!

<u>Szkolenia i vouchery dla 2 pracowników zamawiającego.</u>

3. Termin realizacji zamówienia:

3.1. Zadanie 2.1 (Audyt wstępny Urzędu) - do 40 dni od dnia zawarcia umowy.
3.2. Zadanie 2.2 (analiza ryzyka) i 2.3 (wskazanie obszarów wymagających dostosowania) – do 40 dni do dnia zawarcia umowy.
3.3. Zadanie 2.3 (dokumentacji SZBI) - 2.5 (szkolenia) – do 90 dni od dnia zawarcia umowy – uwzględniając zmiany techniczne realizowane w ramach programu Cyberbezpieczny Samorząd.
3.4. Zadanie 2.4. Przeprowadzenie szkoleń z zakresu zarządzania bezpieczeństwem informacji do 30 od odbioru dokumentacja SZBI przez Zamawiajacego.
3.5.
3.6. Zadanie 2.5 (audytu końcowy) – do 30 dni po zakończeniu realizacji projektu Cyberbezpieczny Samorząd przez Zamawiającego – termin liczony od momentu przekazania informacji przez Zamawiającego o konieczności realizacji niniejszego punktu.
3.7. Zadanie 2.6 (Audyt KRI/UoKSC za rok 2025) od 1 czerwca do 30 września 2025
3.8. Zadanie 2.7 (testy socjotechniczne) – do 30 czerwca 2025.
3.9. Zadanie 2.8 (Microsoft Unlimited) – do stycznia do grudnia 2025

4. Okres gwarancji: nie dotyczy
5. Warunki płatności:

Zamawiający przewiduje płatności częściowe po wykonaniu każdej zadania w ramach realizacji zamówienia zgodnie z zaoferowaną stawką.

Płatność przelewem 30 dni od dnia otrzymania prawidłowo wystawionych faktury VAT wraz z protokołem odbioru konkretnego zadania – protokół potwierdzony przez przedstawiciela Zamawiającego.

6. Inne istotne warunki zamówienia:

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają łącznie warunki:

6.1.1. W okresie ostatnich trzech lat wykonali usługi przygotowania dokumentacji systemu zarządzania bezpieczeństwem informacji w co najmniej czterech organizacjach

zatrudniających powyżej 90 osób, w tym w co najmniej dwóch urzędach administracji publicznej.

6.1.2. W okresie ostatnich trzech lat wykonali usługi audytu ISO/IEC 27001 oraz zgodności z ustawą o krajowym systemie cyberbezpieczeństwa w co najmniej czterech organizacjach zatrudniających powyżej 90 osób, w tym w co najmniej dwóch urzędach administracji publicznej.

6.1.3. W okresie ostatnich trzech lat wykonali usługi audytu KRI w tym zbadanie podatności infrastruktury publicznie dostępnej z Internetu oraz zbadanie podatności infrastruktury sieciowej wewnątrz organizacji (testy penetracyjne) w co najmniej czterech organizacjach zatrudniających powyżej 90 osób, w tym w co najmniej dwóch urzędach administracji publicznej.

6.1.4. W okresie ostatnich trzech lat wykonali usługi doradczej w zakresie cyberbezpieczeństwa w co najmniej trzech organizacjach zatrudniających powyżej 90 osób, w tym w co najmniej dwóch urzędach administracji publicznej.

6.1.5. W okresie ostatnich trzech lat wykonali usługę szkoleniową w zakresie cyberbezpieczeństwa w co najmniej czterech organizacjach zatrudniających powyżej 90 osób, w tym w co najmniej dwóch urzędach administracji publicznej.

6.1.6. Dysponują na podstawie umowy o pracę, samozatrudnienia co najmniej 1 osobom, które posiadają od minimum dwa lat certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PNEN ISO/IEC 27001 oraz certyfikat Zarządzania Ciągłością Działania zgodnie z normą ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku – osoby te w okresie ostatnich trzech lat uczestniczyły w co najmniej czterech audytach systemów zarządzania bezpieczeństwem informacji w organizacjach zatrudniających powyżej 90 osób, w tym w co najmniej dwóch urzędach administracji publicznej.

6.1.7. Dysponują na podstawie umowy o pracę, samozatrudnienia co najmniej jedną osobą będącą specjalistą ds. bezpieczeństwa systemów teleinformatycznych (cyberbezpieczeństwa), posiadającą od minimum dwuch lat co najmniej jeden z certyfikatów o których mowa w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu oraz posiada dodatkowo co najemnie 3 certyfikatów ukończenia certyfikowanych szkoleń z zakresu systemów operacyjnych w tym serwerowych, systemów chmurowych, bazodanowych (np. Windows Serwer, Azure, AD, SQL, SAP) oraz w okresie trzech ostatnich trzech lat brała czynny udział w co najmniej czterech usługach audytu ISO 27001.

6.1.8. Posiadają ważną polisę OC w zakresie prowadzonej działalności w wysokości min. 200 000 zł.

Potwierdzeniem spełnienia wymagań będą referencje lub inne dokumenty potwierdzone przez odbiorcę usługi (protokoły odbioru) jednoznacznie wskazujące należyte wykonanie danej usługi jak również certyfikaty, dyplomy w wymaganym zakresie. Dokumenty należy dołączyć do oferty z wskazaniem spełnienia warunków jakiego punktu dotyczą.

7. Kryterium oceny ofert: cena 100%.
8. Zamawiający informuje, że:
   1.1. Zadania 2.5, 2.6, 2.7, 2.8, 2.9 mogą zostać wyodrębnione jako odrębne części w ramach realizacji zamówienia,
   1.2. w toku badania i oceny ofert może żądać od Wykonawcy pisemnych wyjaśnień dotyczących treści złożonej oferty lub innych składanych dokumentów lub oświadczeń. Wykonawca będzie zobowiązanych do przestawienia wyjaśnień w terminie określonym przez Zamawiającego pod rygorem odrzucenia oferty.
   1.3. wymaga, żeby w każdym etapie realizacji zadania 2.4 uczestniczyła co najmniej jedna osoba, posiadająca kwalifikacje, o których mowa w pkt. 6.1.7,
   1.4. wymaga prowadzenia prac w sposób systematyczny,
   1.5. wymaga, żeby wszystkie dokumenty i cała korespondencja były w j. polskim,
   1.6. przewiduje możliwość zmiany terminu wykonania umowy lub jej zakresu
   1.7. na wszystkich etapach prac Zamawiający zobowiązuje się do współdziałania z Wykonawcą i przekazywania niezbędnych dokumentów, informacji i wyjaśnień,
9. Sposób przygotowania oferty:
   9.1. Ofertę należy sporządzić w języku polskim, na formularzu określonym w załączniku nr 1 do niniejszego zapytania ofertowego i złożyć za pośrednictwem bazy konkurencyjności.
   9.2. Do oferty należy dołączyć certyfikaty oraz referencje potwierdzające spełnienie wymagań.
   9.3. formularz oferty oraz załączniki muszą być podpisane elektronicznie przez osobę upoważnioną do reprezentowania Wykonawcy.
10. **Ofertę należy złożyć w terminie do dnia 24 września 2024 r. do godz. 12:00.**

Stanisław Józef Legierski

Elektronicznie podpisany przez Stanisław Józef Legierski
Data: 2024.09.16 14:54:57 +02'00'