Załącznik nr 3 do zapytania ofertowego nr 19/2024

Nazwa wykonawcy: …………………………………………

**Numer oferty:**

(nadaje zamawiający)

Adres wykonawcy: …………………………………………

 …………………………………………

NIP ……………………

REGON ………………….

Telefon: ……………… Faks: ………………

E-mail: ………………………@………………

**OFERTA**

W związku z zapytaniem ofertowym nr **19/2024** dotyczącym postępowania na udzielenie zamówienia publicznego o wartości mniejszej niż 130 000 złotych na wykonanie w **Rządowym Centrum Bezpieczeństwa audytu w zakresie Krajowych Ram Interoperacyjności poszerzonego o aspekty
z Krajowego Systemu Cyberbezpieczeństwa wraz w przeprowadzeniem diagnozy cyberbezpieczeństwa** przedkładamy ofertę na poniższych warunkach:

1. Oferujemy wykonanie przedmiotu zamówienia zgodnie z poniższymi wymaganiami:

| Lp. | Nazwa elementu | Wymagane minimalne  | spełnia lub nie spełnia |
| --- | --- | --- | --- |
|  | Wymogi podstawowe. | 1. Audyt musi być wykonywany stacjonarnie u Zamawiającego
2. Audyt ma zostać przeprowadzony przez zespół z udziałem co najmniej dwóch audytorów,
3. Cały proces audytowy ma zakończyć się przedstawieniem protokołu (raportu) poaudytowego, zawierającego co najmniej takie elementy jak:
4. definicje prawne;
5. cel audytu;
6. zasada przeprowadzanego audytu;
7. kryteria audytu oraz mierniki oceny;
8. wyniki przeprowadzonego audytu uwzględniając obszary z pkt 2 wraz z opisem obszarów zgodnych w zakresie wymogów KRI;
9. krytycznych niezgodności, szczególnie wpływających na bezpieczeństwo informacji obszarów audytowych wymagających zmiany oraz doskonalenia;
10. wdrożenia procesów poaudytowych mających na celu bieżące i przyszłościowe utrzymanie bezpieczeństwa informacji i systemów IT na poziomie gwarantującym zgodność z KRI;
11. zalecenia w zakresie potencjalnych niezgodności;
12. określenie zakresu i priorytetu działań naprawczych;
13. Wraz z protokołem (raportem) wyniki oraz ocenę audytu przedstawić na spotkaniu kierownictwu Zamawiającego.
 |  |
|  | Zakres audytu. | Audyt ma obejmować obszar:1. działań projektowych, wdrożeniowych oraz eksploatacyjnych z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk;
2. Systemu Zarządzania Bezpieczeństwem Informacji pod kątem poufności, dostępności i integralności;
3. regulacji wewnętrznych w zakresie zmieniającego się otoczenia pod kątem ich aktualizacji;
4. utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
5. okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
6. działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
7. procesów zapewniających szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
* zagrożenia bezpieczeństwa informacji,
* skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
* stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.
1. ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, pod kątem:
* monitorowania dostępu do informacji,
* czynności zmierzających do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
* zapewnienia środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
1. ustanowionych podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
2. zabezpieczeń informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
3. umów serwisowych podpisanych ze stronami trzecimi, gwarantujących odpowiedni poziom bezpieczeństwa informacji;
4. zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
5. odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
* dbałości o aktualizację oprogramowania,
* minimalizowaniu ryzyka utraty informacji w wyniku awarii,
* ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
* stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
* zapewnieniu bezpieczeństwa plików systemowych,
* redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
* niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
* kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
1. poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii;
2. komunikowania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
3. ciągłości wykonywania audytu wewnętrznego (kontroli wewnętrznej);
4. występowania dodatkowych zabezpieczeń, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych;
5. prowadzenia/występowania dzienników systemowych odnotowujących działania użytkowników lub obiektów systemowych, polegających na dostępie do:
* systemu z uprawnieniami administracyjnymi,
* konfiguracji systemu, w tym konfiguracji zabezpieczeń,
* przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa;
1. występowania procedur mogących stanowić odnotowywanie działań użytkowników lub obiektów systemowych, a także innych zdarzeń związanych z eksploatacją systemu w postaci:
* działań użytkowników nieposiadających uprawnień administracyjnych,
* zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu,
* zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny,
* w zakresie wynikającym z analizy ryzyka;
1. procedur związanych z dziennikami systemowymi.
 |  |
|  | Minimalny zakres przedmiotowy audytu - systemy teleinformatyczne oraz usługi | Wykaz systemów IT oraz usług podlegających audytowi: Serwery z rodziny Windows i Linux. 14 serwerów fizycznych, 40 serwerów wirtualnych;1. DMZ – ocena segmentacji sieci;
2. Sieć LAN z serwerami i usługami sieciowymi – switche; routery/firewale, urządzenia ochrony poczty elektronicznej, kontrolery domeny, serwery pocztowe, serwery bazodanowe, serwery usługowe;
3. Zabezpieczenia usług i systemów RCB. - routery/firewale, urządzenia ochrony poczty elektronicznej, systemy antywirusowe, systemy kontroli VPN, analizatory sieci, skanowanie usług, portów, podatności – **z wyłączeniem aktywnego sprawdzania podatności**. (Testy tego typu można przeprowadzić jedynie na kopiach maszyn produkcyjnych);
4. Poczta elektroniczna obsługiwana za pomocą programu Microsoft Exchange OnPremise z klientem Office Outlook firmy Microsoft wraz z systemem antywirusowym, antyspamowym;
5. Usługa w ePUAP – skrzynka podawcza Elektronicznej Platformy Usług Administracji Publicznej, w tym podpisy elektroniczne;
6. System EZD „Edicta” – system do Elektronicznego Zarządzania Dokumentami. Dostarczony i wspierany przez ZETO, w tym podpisy elektroniczne. System pracuje w architekturze klient-serwer;
7. System teleinformatyczny z programem „Kadry i Płace” (zarządzanie dokumentami powiązanymi z poszczególnymi pracownikami);
8. System teleinformatyczny z programem „Płatnik” – (dedykowane oprogramowanie do tworzenie i weryfikacja dokumentów ubezpieczeniowych oraz wymiana informacji z Zakładem Ubezpieczeń Społecznych);
9. Stanowisko platformy Usług Elektronicznych (PUE) ZUS – (oprogramowanie do generowania i przesyłania drogą elektroniczną dokumentów zgłoszeniowych i rozliczeniowych oraz różnego typu pism i wniosków);
10. Stanowisko systemu „Bankowość Elektroniczna NBP”- (oprogramowanie do wspomaga obsługi rachunków bankowych);
11. System teleinformatyczny z programem „Księgowość Budżetowa i Planowanie” – (usprawnia realizację zadań związanych z ewidencją i rozliczeniem budżetu);
12. Program „Środki Trwałe” – (składnik majątku firmowego przewidziany do użytkowania powyżej jednego roku);
 |  |
|  | Minimalne wymogi, audytorów ze składu zespołu audytowego | Audytorzy powinni posiadać uprawnienia:1. audytora wiodącego Systemów Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001:2017 (certyfikacja uzyskana w jednostce akredytowanej przez Polskie Centrum Akredytacji), oraz/lub,
2. audytora wiodącego Systemów Zarządzania Ciągłością; Działania wg normy PN-EN ISO 22301:2020 (certyfikacja uzyskana w jednostce akredytowanej przez CQI & IRCA), oraz/lub,
3. certyfikat określony w rozporządzeniu Ministra Cyfryzacji z dnia 12.10.2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu;
4. Audytorzy powinni wykazać się przeprowadzeniem co najmniej 3 audytów w zakresie KRI.
 |  |

1. Oferujemy wykonanie przedmiotu zamówienia w pełnym zakresie zgodnie z zaproszeniem do składania ofert za cenę brutto:……………… zł

(słownie złotych: …………………………………………………………………….……..…),

w tym podatek VAT w kwocie: ……………… zł\*\*

***W przypadku gdy kwota netto jest równa kwocie brutto.***

Oświadczamy, że przedmiot zamówienia (wykonawca) jest zwolniony z podatku VAT na podstawie …………………………………………………………………………………

1. Zobowiązujemy się wykonywać audyt do dnia ………………..,(maksymalnie do 18.12.2024 r.).
2. Przedmiot zamówienia zamierzamy zrealizować *bez udziału / z udziałem*\* podwykonawców

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

1. Oświadczamy, że:
2. zapoznaliśmy się z warunkami określonymi w Zapytaniu ofertowym (w tym z istotnymi postanowieniami umowy) oraz zdobyliśmy wszelkie informacje konieczne do przygotowania oferty i przyjmujemy warunki w nim określone;
3. akceptujemy warunki płatności zawarte w istotnych postanowieniach umowy;
4. zdobyliśmy konieczne informacje potrzebne do właściwego wykonania zamówienia a wszelkie prace ujęte w ofercie zostały oszacowane w sposób kompleksowy i obejmują wszystkie koszty związane
z prawidłową realizacja usługi;
5. wyrażamy zgodę na dokonanie przez Zamawiającego zamówienia według cen zawartych w niniejszej ofercie zgodnie z zapisami zawartymi w Zapytaniu ofertowym;
6. znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej prawidłowe wykonanie usługi.
7. audytorzy wskazani w złączniku nr 1 do Oferty posiadają wymagane kwalifikacje oraz certyfikaty określone w zapytaniu ofertowym.
8. uważamy się za związanych ofertą przez okres 30 dni od upływu terminu składania ofert;
9. w razie wybrania przez zamawiającego naszej oferty zobowiązujemy się do podpisania umowy
na warunkach zawartych w zaproszeniu do składania ofert oraz w miejscu i terminie określonym przez zamawiającego;
10. na dzień składania oferty *nie podlegamy*\**/ podlegamy*\* wykluczeniu 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.
11. Osoba uprawniona do kontaktów z Zamawiającym:

Imię i Nazwisko……………………….., tel. ……………….., e-mail: …………………………

6. Oferta składa się z ……… kolejno ponumerowanych stron.

7. Załącznikami do niniejszej oferty, stanowiącymi jej integralną część są:

Załącznik nr 1 - wykaz osób skierowanych do realizacji audytu KRI w RCB,

Załącznik nr 2 …………………………………………………,

Załącznik nr 3 …………………………………………………,

Załącznik nr 4 …………………………………………………,

Załącznik nr 5 ………………………………………………….

|  |  |
| --- | --- |
| ……………………………… | ……………………………………… |
| Miejscowość i data | Podpis (podpisy) osób uprawnionychdo reprezentowania Wykonawcy |

*\* - niepotrzebne skreślić*

*\*\* - jeżeli wystąpi konieczność aby Wykonawca podał wartość poszczególnych elementów składających się na kwoty wyżej, można zastosować układ tabelaryczny.*