**ZAPYTANIE OFERTOWE**

Samodzielny Publiczny Zakład Opieki Zdrowotnej w Augustowie zaprasza do złożenia oferty w postępowaniu o wartości szacunkowej nieprzekraczającej 130 000 PLN netto, do którego nie stosuje się przepisów ustawy Prawo zamówień publicznych z dnia 11 września 2019r. (Dz. U. z 2022, poz. 1710 z późn. zm.) na wykonanie audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Przedmiot zamówienia jest podzielony na 2 części. Zamawiający nie dopuszcza składania ofert częściowych.

**Zadanie nr 1**

1. Przedmiotem zamówienia jest usługa przeprowadzenia audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, zwanego dalej "audytem" u operatora usługi kluczowej zgodnie z wymogami ustawy o krajowym systemie cyberbezpieczeństwa oraz aktów powiązanych pod kątem ich zgodności z przepisami oraz normami, o których mowa poniżej oraz przygotowanie i przekazanie Zamawiającemu pisemnego sprawozdania z przeprowadzonego audytu wraz z dokumentacją z przeprowadzonego audytu, zwanego dalej „raportem”.
2. Na podstawie zebranych dokumentów i dowodów audytorzy sporządzą pisemne sprawozdanie z przeprowadzonego audytu zgodne z szablonem sprawozdania z audytu zgodnego z ustawą KSC, opracowanym przez Ekspertów z ISSA Polska - Stowarzyszenia do spraw Bezpieczeństwa Systemów Informacyjnych oraz IIA Polska - Instytutu Audytorów Wewnętrznych pod nadzorem ówczesnego Ministerstwa Cyfryzacji (https://www.gov.pl/web/baza-wiedzy/szablony-audytu-dla-operatorow-uslug-kluczowych)
3. Celem audytu jest potwierdzenie zgodności bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia Usług Kluczowych z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa.
4. Ocena bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług kluczowych realizowanych przez Szpital oraz identyfikacja i analiza luki zgodności z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa przeprowadzona powinna zostać w oparciu o 10 obszarów tj.:

Obszar 1: Organizacja zarządzania bezpieczeństwem informacji

Obszar 2: Procesy zarządzania bezpieczeństwem informacji

Obszar 3: Zarządzanie ryzykiem

Obszar 4: Monitorowanie i reagowanie na incydenty bezpieczeństwa

Obszar 5: Zarządzanie zmianą

Obszar 6: Zarządzanie ciągłością działania

Obszar 7: Utrzymanie systemów informacyjnych

Obszar 8: Utrzymanie i rozwój systemów informacyjnych

Obszar 9: Bezpieczeństwo fizyczne

Obszar 10: Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług

1. Warunki udziału w postępowaniu :
2. Audyt bezpieczeństwa, o którym mowa może być przeprowadzony przez:

1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;

2) co najmniej dwóch audytorów posiadających:

a) certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu (każdy z audytorów powinien posiadać przynajmniej po jednym z wymienionych certyfikatów) lub

b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub

c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.

Wykaz certyfikatów uprawniających do przeprowadzenia audytu

1) Certified Internal Auditor (CIA),

2) Certified Information System Auditor (CISA),

3) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób,

4) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN 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, w zakresie certyfikacji osób,

5) Certified Information Security Manager (CISM)

6) Certified in Risk and Information Systems Control (CRISC)

7) Certified in the Governance of Enterprise IT (CGEIT)

8) Certified Information Systems Security Professional (CISSP)

9) Systems Security Certified Practitioner (SSCP)

10) Certified Reliability Professional 11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

1. Termin realizacji zamówienia

Sporządzenie pisemnego z przeprowadzonego audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej i doręczenie go Zamawiającemu do dnia 19 lipca 2023r.

**Zadanie nr 2**

Samodzielny Publiczny Zakład Opieki Zdrowotnej w Augustowie zaprasza do złożenia oferty w postępowaniu o wartości szacunkowej nieprzekraczającej 130 000 PLN netto, do którego nie stosuje się przepisów ustawy Prawo zamówień publicznych z dnia 11 września 2019r. (Dz. U. z 2019, poz. 2019 z późn. zm.j na:

**„Wykonanie uzupełniającego audytu bezpieczeństwa na potrzeby i na podstawie „ZARZĄDZENIA NR 8/2023/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA z dnia 16 stycznia 2023 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców"**

1. Opis przedmiotu zamówienia
2. Przedmiotem zamówienia jest wykonanie audytu bezpieczeństwa systemów teleinformatycznych Zamawiającego (dalej jako „Audyt") oraz sporządzenie raportu z audytu z wynikami wykonanych czynności (zwanego dalej: „Raportem"), którego szczegółowy zakres określa Załącznik nr 1 do Zapytania Ofertowego.
3. Celem audytu jest dokonanie oceny poziomu bezpieczeństwa teleinformatycznego Zamawiającego po zrealizowaniu czynności, które mogą zostać objęte finansowaniem zgodnie z ZARZĄDZENIEM NR 8/2023/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA z dnia 16 stycznia 2023 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców.
4. Z Przeprowadzonego Audytu Wykonawca sporządzi Raport, z którego będzie wynikać podniesienie poziomu bezpieczeństwa teleinformatycznego Zamawiającego w odniesieniu do poziomu wynikającego z „Ankiety weryfikacji dojrzałości pod kątem bezpieczeństwa" lub jego brak.
5. Termin realizacji zamówienia

Audyt przeprowadzony musi zostać w terminie od 20 lipca 2023 do 20 sierpnia 2023. Sporządzenie pisemnego Raportu z Audytu poziomu bezpieczeństwa teleinformatycznego Zamawiającego i doręczenie go Zamawiającemu nastąpi do dnia 30 sierpnia 2023r.

1. Miejsce i termin złożenia oferty

Ofertę w formie elektronicznej należy przesłać drogą elektroniczną na adres e-mail : zp@spzoz.augustow.pl w terminie 04.07.2023 r. W skład oferty wchodzi formularz ofertowy ( załącznik nr 2 do zapytania ofertowego ) i oświadczenie o braku powiązań kapitałowych lub osobowych ( załącznik nr 3 do zapytania ofertowego ).

1. Dokumenty potwierdzające spełnianie warunków udziału w postępowaniu

Zamawiający wezwie Wykonawcę, którego oferta zostanie najwyżej oceniona do złożenia w terminie 2 dni kserokopii certyfikatów potwierdzonych za zgodność z oryginałem lub oświadczenia o spełnianiu wymogu posiadania co najmniej trzyletniej praktyki z zakresu audytu systemów informacyjnych lub oświadczenia o spełnianiu wymogu posiadania co najmniej dwuletniej praktyki z zakresu audytu systemów informacyjnych i kserokopii potwierdzonej za zgodność z oryginałem dyplomu ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.

1. Kryteria oceny ofert :

Cena – 100 punktów.

Załączniki do zapytania ofertowego :

Załącznik nr 1 – obszary audytu

Załącznik nr 2 – formularz oferty

Załącznik nr 3 – oświadczenie o braku powiązań kapitałowych lub osobowych

Załącznik nr 4 – projekt umowy

Załącznik nr 1 do zapytania ofertowego

|  |  |
| --- | --- |
| Nazwa obszaru | Opis działań skutkujących podniesieniu poziomem bezpieczeństwa teleinformatycznego u świadczeniodawców  |
| Skuteczność działania infrastruktury | - Urządzenia i konfiguracja w zakresie ochrony poczty - Urządzenia i konfiguracja w zakresie ochrony sieci - Urządzenia i konfiguracja w zakresie systemów serwerowych - Urządzenia i konfiguracja w zakresie stacji roboczych - Urządzenia i konfiguracja w zakresie systemów bezpieczeństwa  |
| Procesy zarządzania bezpieczeństwem informacji | - Nośniki wymienne - udokumentowany sposób postępowania - Zarządzanie tożsamością / dostęp do systemów w zakresie:  - Przydzielanie dostępu  - Odbieranie dostępu - Pomieszczenie w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeństwo w przypadku podmiotów, które otrzymały decyzję uznającą taki podmiot za operatora usługi kluczowej, o którym mowa w art. 5 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa  |
| Monitorowanie i reagowanie na incydenty bezpieczeństwa | - Procedury zarządzania incydentami - Raportowanie poziomów pokrycia scenariuszami znanych incydentów - Dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego/ sektorowego zespołu cyberbezpieczeństwa - Monitorowanie i wykrycie incydentów bezpieczeństwa - Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów |
| Zarządzanie ciągłością działania | - Konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa - Raport z przeglądów i testów odtwarzania kopii bezpieczeństwa - Procedury wykonywania i przechowywania kopii zapasowych - Strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP) - Procedury utrzymaniowe |
| Utrzymanie systemów informacyjnych | - Harmonogramy skanowania podatności - Aktualny status realizacji postępowania z podatnościami - Procedury związane ze z identyfikowaniem (wykryciem) podatności - Współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami  |
| Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług | - Polityka bezpieczeństwa w relacjach z dostawcami - Standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa - Dostęp zdalny - Metody uwierzytelnienia |

**OBOWIĄZEK INFORMACYJNY DOTYCZĄCY DANYCH PRZETWARZANYCH**

**W ZWIĄZKU Z ZAPYTANIEM OFERTOWYM**

Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, RODO) informuję, że:

1. Administratorem Pana/Pani danych osobowych jest Samodzielny Publiczny Zakład Opieki Zdrowotnej w Augustowie ul. Szpitalna 12, 16-300 Augustów.
2. Administrator, zgodnie z art. 37 ust. 1 lit. a) RODO, powołał Inspektora Ochrony Danych, z którym możecie Państwo kontaktować się pod adresem poczty elektronicznej: iod@spzoz.augustow.pl.
3. Dane osobowe przetwarzane będą:
* na etapie postępowania o udzielenie zamówienia: na podstawie art. 6 ust. 1 lit. c RODO w związku z art. 43 i 44 ustawy o finansach publicznych w celu związanym z postępowaniem o udzielenie zamówienia publicznego poniżej 30000 euro;
* na etapie zawierania umowy: na podstawie art. 6 ust. 1 lit. b RODO w celu związanym z udzielanym zamówieniem publicznym poniżej 30000 euro tj.: w celu zawarcia i prawidłowego wykonania umowy.
1. Administrator gwarantuje, że Państwa dane są przetwarzane w minimalnym zakresie umożliwiającym realizację ściśle określonego celu.
2. Odbiorcami danych osobowych mogą być: podmioty uprawnione do uzyskania danych na podstawie przepisów prawa lub podpisanych umów powierzenia przetwarzania danych, osoby upoważnione przez Administratora, operatorzy pocztowi, podmioty realizujące archiwizację, obsługa informatyczna i teleinformatyczna.
3. Dane osobowe będą przetwarzane do czasu osiągnięcia celu, w jakim je pozyskano, a po tym czasie przez okres oraz w zakresie wymaganym przez przepisy powszechnie obowiązującego prawa.
4. Przysługuje Państwu, w zależności od charakteru przetwarzania, prawo dostępu do treści swoich danych osobowych oraz prawo żądania ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do sprzeciwu, prawo do przenoszenia danych, a także prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych. Dodatkowo w przypadku, gdy podstawą przetwarzania Państwa danych osobowych jest Państwa dobrowolna zgoda, przysługuje Państwu prawo do cofnięcia wyrażonej zgody w dowolnym momencie.
5. Podanie przez danych osobowych jest obowiązkowe. W przypadku niepodania danych nie będzie możliwe zawarcie umowy o udzielenie zamówienia poniżej 30 000 euro.
6. Państwa dane osobowe nie będą wykorzystywane do zautomatyzowanego podejmowania decyzji ani profilowania, o którym mowa w art. 22 RODO.