Przeprowadzenie audytu zgodności z ustawą o Krajowym Systemie Cyberbezpieczeństwa

Numer ogłoszenia: II.0400.1.2022

Data zamieszczenia: 24.10.2022

Zamawiający : Krakowski Szpital Specjalistyczny im. Jana Pawła II , ul. Prądnicka 80, 31-202 Kraków

A.Informacje dotyczące zamówienia:

1) **Miejsce składania ofert:**
   - Ofertę można złożyć w formie pisemnej/ w zamkniętej kopercie lub innym opakowaniu , wyraźnie oznaczonej numerem postępowania/ w siedzibie Zamawiającego przy ul. Prądnickiej **80** w Krakowie w budynku Administracyjno-Konferencyjnym - Pawilon A-V (Dziennik Podawczy) lub **na Platformie zakupowej,** do **dnia 07.11.2022 , do godziny 9:00.** Oferty złożone po terminie nie będą otwierane i zostaną niezwłocznie zwrócone Wykonawcy.
2) **Prowadzone postępowanie nie stanowi przetargu w rozumieniu Kodeksu cywilnego ani ustawy Prawo Zamówień Publicznych. Zamawiający nie jest zobligowany do wyboru jakiejkolwiek oferty, a złożenie oferty nie stanowi podstawy do występowania z jakimkolwiek roszczeniami wobec Zamawiającego ze strony podmiotu, który złożył ofertę**.
3) **Warunki zgłaszania ofert:**
   - Wykonawca musi posiadać uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania.
   - Wykonawca posiada wiedzę i doświadczenie odpowiednie do wykonania zamówienia.
   - Wykonawca może zaproponować tylko jedną cenę i nie może jej zmienić,
   - Oferta zawiera datę końcową związania ofertą, nie krótszą niż 3 tygodnie od daty złożenia oferty,

- Wykonawca zobowiązany jest potwierdzić ,że nie zachodzą przesłanki wykluczenia z postępowania na podstawie art.7 ust.1 w zw. Z art.7 ust.9 ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.
- W związku z treścią art. 5k ROZPORZĄDZENIA RADY (UE) NR 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie Wykonawca jest zobowiązany zapewnić aby przez cały okres obowiązywania umowy z Zamawiającym nie podlegał pod sankcje opisaną w wyżej wymienionym przepisie. W wypadku zaistnienia którejkolwiek z przesłanek opisanych w wyżej wymienionym artykule skutkujących zakazem dalszego wykonywania wszelkich zamówień publicznych w jego rozumieniu Wykonawca zobligowany jest do natychmiastowego zawiadomienia o tym fakcie Zamawiającego.

- Zamawiający nie jest zobligowany do wyboru jakiejkolwiek oferty, a złożenie oferty nie stanowi podstawy do występowania z jakimkolwiek roszczeniem wobec Zamawiającego ze strony podmiotu który złożył ofertę. W szczególności, Zamawiający nie dokonuje wyboru ofert, jeżeli:
  a).oferta z najkorzystniejszą ceną przekracza kwotę, którą zamawiający zamierza przeznaczyć na sfinansowanie zamówienia,
  b).wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonania zamówienia nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć

4) Oferta wraz z załącznikami musi być podpisana przez osobę/osoby uprawnione do składania oświadczeń woli w imieniu wykonawcy zgodnie z zasadami reprezentacji. Jeżeli osoba/ osoby podpisująca ofertę działa na podstawie pełnomocnictwa, to pełnomocnictwo to musi w swej treści jednoznacznie wskazywać uprawnienie do podpisania oferty. Pełnomocnictwo to musi być dołączone do oferty i musi być złożone w oryginale lub kopii poświadczonej za zgodność z oryginałem przez osobę wymienioną w rejestrze, która jest wskazana, jako upoważniona do reprezentowania Wykonawcy lub przez

notariusza.

5) Oferta musi być sporządzona w języku polskim. Każdy dokument składający się na ofertę sporządzony w innym języku niż język polski powinien być złożony wraz z tłumaczeniem na język polski.

Wykonawca zobowiązany jest do podpisania umowy, której wzór jest załącznikiem do niniejszego postępowania

B. Wymagania dotyczące audytu:

Oferta ma dotyczyć przeprowadzenia audytu "zerowego" i końcowego oraz szkoleń z zagrożeń i bezpieczeństwa dla pracowników Szpitala, najlepiej w przystępnej formie filmików instruktażowych zakończonych quiz'em sprawdzającym.
Audyt musi być przeprowadzony **zgodnie** z **zarządzeniem Prezesa Narodowego Funduszu Zdrowia NR 68/2022/BBIICD**.
Podczas przeprowadzenia audytu nie może dojść do spowolnienia, zatrzymania czy uszkodzenia jakichkolwiek systemów Szpitala. Audyt nie może wpłynąć na bieżącą pracę Szpitala.

Planowany termin audytu to listopad 2022 r.

Szkolenia powinny dotyczyć tematyki:

a) zagrożeń w cyberprzestrzeni
b) mechanizmów wykorzystania metod socjotechnicznych
c) omówienie Phishingu z przykładami ataków
d) korzystanie z mediów społecznościowych w sposób bezpieczny (omówienie jakie dane o nas dostępne są w sieci)
e) używanie mocnych haseł do systemów
f) ransomware - co to jest i jakie są zagrożenia. Jak się zabezpieczyć przed atakami
g) praca zdalna (VPN i inne metody dostępu) - bezpieczeństwo zdalnej pracy.

Wymagania dotyczące audytu bezpieczeństwa

Audyt bezpieczeństwa, o którym mowa w niniejszego zarządzenia 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 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 Intemal Auditor (CIA);

1) Certified Information System Auditor (CISA);

2) 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,* w zakresie certyfikacji osób;

3) 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;

4) Certified Information Security Manager (CISM);

5) Certified in Risk and Information Systems Control (CRISC);

6) Certified in the Govemance of Enterprise IT (CGEIT);

7) Certified Information Systems Security Professional (CISSP);

8) Systems Security Certified Practitioner (SSCP);

9) Certified Reliability Professional;

10) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

Celem audytu jest wykazanie przez świadczeniodawcę podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności, zgodnie z niniejszym zarządzeniem oraz w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u świadczeniodawcy w formie ankiety. Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa.

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

Tel. kontaktowy: 12/614 24 17