OPIS PRZEDMIOTU ZAMÓWIENIA

Wykonanie audytu bezpieczeństwa potwierdzającego zwiększenie poziomu bezpieczeństwa teleinformatycznego u Zamawiającego

**ZAKRES**

Celem audytu jest potwierdzenie wymagań wobec operatora usługi kluczowej określonych w **Ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa** oraz wykazanie podniesienia poziomu bezpieczeństwa teleinformatycznego przez Zamawiającego po zrealizowaniu czynności, zgodnie z **Zarządzeniem nr 68/2022/BBIICD** Prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców oraz
w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u świadczeniodawcy w formie ankiety. Przeprowadzony audyt musi wykazać podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety albo jego brak.

Wykonawca na zakończenie przedstawi 2 raporty z audytu:

1. **Raport pierwszy** musi zawierać jednoznaczne i jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa (zgodnie z **Zarządzeniem nr 68/2022/BBIICD** Prezesa Narodowego Funduszu Zdrowia).
2. **Raport drugi** musi spełniać wymagania dotyczące sprawozdania z przeprowadzenia audytu bezpieczeństwa opisane w **Ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.**

Obszary oceny poziomu bezpieczeństwa teleinformatycznego:

1. 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.
1. 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.
1. 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.
1. 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.
1. 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.
1. 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.

**WYMAGANIA**

O udzielenie zamówienia może ubiegać się wykonawca, który spełnia wymagania dotyczące audytu bezpieczeństwa określone w **zarządzeniu nr 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców** oraz **Ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa** wraz z r**ozporządzeniem Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu**:

1. Jest jednostką 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 (załączyć do oferty kopię certyfikatu akredytacji).
2. Dysponuje co najmniej dwoma audytorami posiadającymi:
* minimum jeden z certyfikatów określonych w poniższym wykazie certyfikatów uprawniających do przeprowadzenia audytu **lub**
* co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych **lub**
* 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.

Sposób potwierdzenia praktyki zgodny z wymaganiami określonymi w Ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

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.
12. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
13. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają usługi, do realizacji których te zdolności są wymagane.
14. Wykonawca, który polega na zdolnościach podmiotów udostępniających zasoby, składa, wraz z ofertą, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
15. W przypadku, o którym mowa w art. 117 ust. 3 ustawy, wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika, które usługi wykonają poszczególni wykonawcy.