Załącznik nr 2 b dla części nr 2
Nr postępowania EZP-252-23/2022

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest:

Zakup i wdrożenie systemów teleinformatycznych oraz usług służących poprawie poziomu cyberbezpieczeństwa.

Część nr 2. Audyt bezpieczeństwa systemów IT

Zamawiający wymaga przeprowadzenia Audytu Bezpieczeństwa, zgodnie z Zarządzeniem Nr 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022 roku w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców.

1. **Audyt bezpieczeństwa należy przeprowadzić w Świętokrzyskim Centrum Psychiatrii w Morawicy**

Zamawiający Informuje, że audytem objęte będzie środowisko składające się z :
1) liczba stacji roboczych (komputerów) – 386
2) liczba serwerów fizycznych 6
3) liczba serwerów wirtualnych 16
4) liczba użytkowanych systemów 902
5) liczba pracowników 902.

2. **Wymagania:**

Audyt bezpieczeństwa może być przeprowadzony przez:
1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016r. 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 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, 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.

3. **Celem audytu jest wykazanie podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności** w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa. 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, czy spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa

4. **Wymagania dla jednostki przeprowadzającej audyt:**

Zamawiający wymaga, aby jednostka przeprowadzająca audyt spełniała wymagania określone w:
- Załączniku nr 2 do Zarządzenia 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 2018r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. 2018 poz. 1560).

5. **Kryteria audytu Bezpieczeństwa oparte będą o:**
   1. Ankietę weryfikacji pod kątem dojrzałości cyberbezpieczeństwa.
   2. Wymagania normatywne PN-EN ISO/IEC 27001:2017-06.
   3. Wymagania normatywne PN-EN ISO 22301:2020-04.
   4. Wewnętrzną dokumentację Zamawiającego.
   5. Przepisy o Krajowym Systemie Cyberbezpieczeństwa.
   6. Standardy Krajowych Ram Interoperacyjności (KRI).

6. Zakresem Audytu objęta będzie cała działalność Zamawiającego.

7. Zamawiający wymaga realizacji usługi w formie stacjonarnej.

8. Wykonawca po przeprowadzeniu audytu przekaże Zamawiającemu kompletny Raport audytu.

9. Do oferty należy dołączyć:
a) Certyfikat wdrożonej normy ISO 27001 i ISO 22301 .

10. **Audyt obejmuje:**

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

.....

podpis
elektroniczny kwalifikowany
lub podpis **zaufany** lub **osobisty**
osoby/-ób uprawnionej/-ych
do reprezentowania Wykonawcy