OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest wykonanie trzyetapowego audytu:

a) Audyt zerowy
b) Przygotowanie dokumentacji
c) Audyt końcowy

Celem audytu jest weryfikacja stanu bieżącego istniejącej infrastruktury IT w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych dla Miejskiego Szpitala Zespolonego w Częstochowie. Audyt ma wykazać obszary w których niezbędne są zmiany konieczne do podniesienia poziomu bezpieczeństwa teleinformatycznego, które zostały opisane w zarządzeniu z dnia 20 maja 2022 r. nr 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia wraz z uwzględnieniem ankiety cyberbezpieczęństwa przesłanej przez szpital do CSIRT. Wykonanie audytu końcowego po realizacji założonych celów.
Wymagania do przeprowadzenia audytu

- Audyt musi zostać przeprowadzony zgodnie z metodyką ISO
- Audyt musi weryfikować poziom bezpieczeństwa teleinformatycznego Zamawiającego
  - W odniesieniu do samooceny poziomu dojrzałości cyberbezpieczeństwa Zamawiającego przeprowadzonej ankietą w systemie CEZ z dnia 12.04.2022
  - W odniesieniu do efektów wpływu na cyberbezpieczeństwo rozwiązań wdrożonych przez Zamawiającego w okresie od maja do grudnia rozwiązań IT (realizowane w ramach osobnych postępowań)
- Niezależnie od powyższego audyt musi spełniać równocześnie wymogi audytu zgodności dla Operatora Usługi Kluczowej zgodnie z wymogami ustawy o Krajowym Systemie Cyberbezpieczeństwa.
- Audyt musi weryfikować zarówno aspekty organizacyjne jak i techniczne :

1. Skuteczność działania infrastruktury,
2. Procesy zarządzania bezpieczeństwem informacji;
3. Monitorowanie i reagowanie na incydenty bezpieczeństwa;
4. Zarządzanie ciągłością działania;
5. Utrzymanie systemów informacyjnych;
6. Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług;

Przedmiot zamówienia należy wykonać zgodnie z aktualnie obowiązującymi przepisami prawa powszechnie obowiązującego, w szczególności opisanych w zarządzeniu z dnia 20 maja 2022 r. nr 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia, załącznikiem nr 2 do umowy nr 123/108020/BEZP o finansowaniu ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców oraz zgodnie z wymogami ustawy o Krajowym Systemie Cyberbezpieczeństwa dla Operatora Usługi Kluczowej.

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 Internal 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 Governance 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.

Oferent musi dysponować w zespole audytowym dedykowanymi specjalistami z obszarów:

- rozwiązań sieciowych
- systemu operacyjnego Windows
- rozwiązań storage'owy
- rozwiązań backup'owych
- wirtualizacji
- rozwiązań klasy EDR
- analizy i zarządzania ryzykiem