



WSzS.DTI.26.5.2022

Częstochowa, dn. 05.07.2022 r.

Szczegółowy opis przedmiotu zamówienia

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.

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

4. W postępowaniu może wziąć udział Wykonawca, który dysponuje zespołem spełniającym wymagania ustawy o krajowym systemie cyberbezpieczeństwa. Audyt musi zostać przeprowadzony przez osobę posiadającą uprawnienia wykazane w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. poz. 1999) w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie

cyberbezpieczeństwa (t.j. Dz. U. z 2020 r. poz. 1369 z późn. zm.). Wykaz certyfikatów wskazanych rozporządzeniu znajduje się poniżej:

- 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
5. Wykonawca musi posiadać doświadczenie w przeprowadzaniu co najmniej 2 usług audytorskich odpowiadających swoim rodzajem usłudze stanowiącej przedmiot zamówienia w przeciągu 4 lat od terminu składania ofert.
6. W celu potwierdzenia spełnienia powyższych wymagań Wykonawca zobowiązany jest do przedłożenia wraz z formularzem oferty wykazu osób przewidzianych do realizacji zamówienia, kopii certyfikatów oraz wykazu zrealizowanych usług audytorskich.
7. Audytorzy zobowiązani są do zachowania w tajemnicy informacji uzyskanych w związku z przeprowadzonym audytem, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych.
8. Podstawowe informacje dotyczące Wojewódzkiego Szpitala Specjalistycznego im. Najświętszej Maryi Panny w Częstochowie
- Posiadane i utrzymywane certyfikaty: ISO 9001:2015
 - Liczba lokalizacji: 2
 - Ogólna liczba pracowników: 2199
 - Liczba pracowników IT: 9 osób
 - Ilość systemów wykorzystywanych do świadczenia usługi kluczowej: 6
 - Liczba stanowisk komputerowych: >700
 - Liczba serwerów fizycznych: 22
 - Liczba serwerów wirtualnych: 25 (docelowo 33)
 - Ilość serwerowni: 2
 - Ilość Access Point (WiFi): 80
 - Ilość podsięci: 4

- Ilość adresów zewnętrznych: 4
- Ilość switchy: 60
- Firewall: Tak
- DHCP: Tak
- IPS: Tak
- SSL VPN Fortigate: Tak
- VPN SSL (Open VPN): Nie
- Drukarki sieciowe: 250
- Ilość urządzeń sieciowych: 380
- Ilość stron internetowych: 3
- Active Directory: Tak
- Ochrona fizyczna i techniczna obiektów: Outsourcing