OPIS PRZEDMIOTU ZAMÓWIENIA

I. Przedmiot zamówienia:

1. Przedmiotem zamówienia jest wykonanie audytu bezpieczeństwa systemów informacyjnych dla Szpitala im. T. Marciniaka Centrum Medycyny Ratunkowej mieszczącego się przy ul. Fieldorfa 2 we Wrocławiu.
2. Szpital zgodnie z wydaną przez Ministerstwo Zdrowia Decyzją posiada 2 usługi kluczowe. Jedna w sposób ogólny odnosi się do udzielania świadczeń opieki zdrowotnej, druga dotyczy obrotu i dystrybucji lekami. Systemy wspierające te dwie usługi kluczowe to HIS (Asseco amms), RIS, PACS (Pixel AlleRad). Systemy te działają w oparciu o środowisko informatyczne wymienione w **załączniku nr 1**.
3. Zamawiający wymaga aby sprawozdanie z audytu było zgodne z wytycznymi zamieszczonymi na stronie: https://mc.bip.gov.pl/krajowy-system-cyberbezpieczenstwa/operatorzy-uslug-kluczowych/szablon-sprawozdania-z-audytu-zgodnego-z-ustawa-o-krajowym-systemie-cyberbezpieczenstwa.html .
4. Zakres przedmiotu zamówienia:

Audyt należy przeprowadzić w oparciu o następujące obszary:

1) Organizacja zarządzania bezpieczeństwem informacji:
   a) Dokumentacja potwierdzająca wykonane działania zgodnie z harmonogramem wskazanym w ustawie KSC (tekst jednolity: Dz. U. z 2020, poz.1369 ze zmianami),
   b) Opis Identyfikacji Systemu Informacyjnego wspierającego Usługę Kluczową,
   c) Dokumentacja Systemu Informacyjnego wspierającego Usługę Kluczową.
2) Procesy zarządzania bezpieczeństwem informacji:
   a) System zarządzania bezpieczeństwem informacji bazujący na ISO-27001,
   b) Pracownicy CSIRT/SOC/DC,
   c) Dostęp do wiedzy z zakresu Cyberbezpieczeństwa (Art. 9.1.2 ustawy KSC) – dokumentacja poświadczająca,
3) Zarządzanie ryzykiem:
   Proces zarządzania ryzykiem Usługi Kluczowej.
4) Monitorowanie i reagowanie na incydenty bezpieczeństwa:
   a) Dokumentacja procesu zarządzania incydentami,
   b) Monitorowanie Cyberbezpieczeństwa,
   c) Poprawność procesu z UKSC.
5) Zarządzanie zmianą:
   Dokumentacja procesu zarządzania zmianą.
6) Zarządzanie ciągłością działania:
   Dokumentacja procesu zarządzania ciągłością działania.
7) Utrzymanie systemów informacyjnych:
   Dokumentacja procesu zarządzania podatnościami i zagrożeniami.
8) Utrzymanie i rozwój systemów informacyjnych:
   Środowisko rozwojowe – dokumentacja.
9) Bezpieczeństwo fizyczne:
   Pomieszczenia CSIRT/SOC/Działu.
10) Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług:

a) Dostawcy OUK – dokumentacja,
b) Dokumentacja Podmiotu Świadczącego Usługi Cyberbezpieczeństwa.

Wykaz systemów objętych audytem zawarty jest w **załączniku nr 1**.

II. Warunki udziału w postępowaniu

Audyt 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 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
2. co najmniej dwóch audytorów z których każdy posiada:
   1) co najmniej jeden z certyfikatów, których wykaz znajduje się w **załączniku nr 2**, **lub**
   2) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, **lub**
   3) 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;

Za praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, o której mowa powyżej, uważa się udokumentowane wykonanie w ciągu ostatnich 3 lat przed dniem rozpoczęcia audytu - 3 audytów w zakresie bezpieczeństwa systemów informacyjnych lub ciągłości działania albo wykonywanie audytów bezpieczeństwa systemów informacyjnych lub ciągłości działania w wymiarze czasu pracy nie mniejszym niż 1/2 etatu, związanych z:

1) przeprowadzaniem audytu wewnętrznego pod nadzorem audytora wewnętrznego;
2) przeprowadzaniem audytu zewnętrznego pod nadzorem audytora wiodącego;
3) przeprowadzaniem audytu wewnętrznego w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
4) wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 15 lipca 2011r. o kontroli w administracji rządowej (Dz. U. poz. 1092);
5) wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2017 r. poz. 524 oraz z 2018 r. poz. 1000).

Zamawiający zastrzega sobie prawo żądania od Wykonawców, na dowolnym etapie postępowania, okazania dokumentów poświadczających spełnianie przez Wykonawcę wskazanych powyżej warunków udziału w postępowaniu.

III. Podstawy wykluczenia z udziału w postępowaniu:

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na podstawie art.7 ust.1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. poz. 835).

IV. Termin realizacji: 21 dni od daty zawarcia umowy.

V. Pozostałe informacje

Szczegółowe warunki realizacji przedmiotu zamówienia zostały zawarte w załączonym wzorze umowy.

Zamawiający wymaga od Wykonawców zawarcia umowy na warunkach określonych w załączonym wzorze umowy.

Załącznik nr 1

WYKAZ SYSTEMÓW OBJĘTYCH AUDYTEM

Środowisko informatyczne składa się z następujących technologii:

1. Platformy Sprzętowe
    a) Serwery HPE Proliant DL360; DL380, Blade System c7000 z serwerami BL460c
    b) Serwery Fujitsu Primergy RX2540
    c) Macierze dyskowe Fujitsu DX100, HP 3PAR 7400c, HP 3PAR 7200c, HP MSA 2050
    d) Przełączniki HPE
    e) Biblioteka taśmowa HPE
3. Platformy wirtualizacyjne
    a) Microsoft Hyper-V
    b) Vmware ESXi
4. Systemy Operacyjne
    a) Microsoft Windows
    b) RedHat Linux
    c) Centos Linux
5. Systemy bazodanowe
    a) Oracle
    b) MS SQL
6. Systemy aplikacyjne
    a) JBoss
    b) Tomcat
7. Systemy Zabezpieczeń
    a) Firewalle Fortigate
    b) AV Eset
    c) SIEM&SOAR SecureVisio

Załącznik nr 2

WYKAZ CERTYFIKATÓW UPRAWNIAJĄCYCH DO PRZEPROWADZANIA 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.