Samodzielny Publiczny Zakład Opieki Zdrowotnej
Wojewódzki Szpital Specjalistyczny nr 4 w Bytomiu
Aleja Legionów 10, 41-902 Bytom, NIP 626-25-10-567, **REGON** 000296271
tel. +48 323 964 500, e-mail: szpital@szpital4.bytom.pl, www.wss4.pl

Załącznik Nr 2E do SWZ (Pakiet Nr 5)

OPIS PRZEDMIOTU ZAMÓWIENIA – PAKIET NR 5

A. DZIAŁANIE

Projekt	101	eCareMed - rozwój cyfrowych usług medycznych w Wojewódzkim Szpitalu Specjalistycznym nr 4 w Bytomiu.
Dział	261	Zamówienia Publiczne.
Katalog	130	Audyt bezpieczeństwa danych – **Pakiet Nr 5**
Element	101	Opis przedmiotu zamówienia.
Wersja	2	2022-05-23

B. WSTĘP

Przedmiotem zamówienia jest usługa polegająca na przeprowadzeniu w Wojewódzkim Szpitalu Specjalistycznym Nr 4 w Bytomiu zewnętrznego audytu bezpieczeństwa infrastruktury teleinformatycznej (audytu cyberbezpieczeństwa) w zakresie:

1. Weryfikacji poziomu spełnienia wymagań Rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
2. Weryfikacji poziomu spełnienia wymagań Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
3. Weryfikacji poziomu spełnienia wymagań regulacji wewnętrznych dotyczących bezpieczeństwa informacji, w tym danych osobowych, zawartych w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji obowiązującym w szpitalu.

C. ZAKRES AUDYTU

1. Organizacyjne środki bezpieczeństwa
   a) Przegląd dokumentacji SZBI w obszarze bezpieczeństwa informacji, w tym danych osobowych.
   b) Weryfikacja procesów i czynności przetwarzania danych uwzględniając ich charakter, zakres, kontekst, cele przetwarzania i ryzyka.
   c) Weryfikacja zasad odpowiedzialności personalnych za funkcjonowanie systemów informatycznych.
   d) Weryfikacja zasad korzystania z dostawców i wykonawców w obszarze systemów informatycznych.
   e) Weryfikacja realizowania przez pracowników obowiązków wynikających z regulacji wewnętrznych – w zakresie bezpieczeństwa informacji, w tym danych osobowych. Weryfikacja musi obejmować przynajmniej kierownika lub zastępcę kierownika każdej komórki organizacyjnej oraz 3 jej pracowników.
2. Fizyczne i środowiskowe środki bezpieczeństwa
   Weryfikacja środków technicznych i środowiskowych służących zabezpieczaniu elementów systemu informatycznego przetwarzających informacje, w tym dane osobowe, w szczególności analiza stanu bezpieczeństwa siedziby (budynków i pomieszczeń) Zamawiającego na podstawie wizji lokalnej.
3. Informatyczne środki bezpieczeństwa
   Audyt informatycznych środków bezpieczeństwa będzie polegał na przeprowadzeniu badania wybranej reprezentatywnej próby elementów systemu informatycznego.
4. Weryfikacja bezpieczeństwa infrastruktury sieciowej, w szczególności:
   a) inwentaryzacja urządzeń sieciowych (adresy IP, konfiguracja urządzeń, konfiguracja zapory ogniowej, podział na sieci logiczne i fizyczne) w siedzibie Zamawiającego,
   b) analiza sposobu połączenia segmentów sieci pomiędzy sobą,
   c) analiza metody komunikacji pomiędzy segmentami sieci,
   d) analiza urządzeń i systemów zapewniających dostęp do sieci Internet (serwera brzegowego, urządzeń UTM, firewall, routerów, itp.) pod kątem:
      – ochrony przed zagrożeniami z sieci Internet,
      – bezpieczeństwa udostępniania w Internecie usług,
      – bezpieczeństwo sieci Wi-Fi,
      – dostępu zdalnego do sieci komputerowej,
      – połączeń pomiędzy jednostkami organizacyjnymi Zamawiającego i podmiotami zewnętrznymi.
5. Weryfikacja bezpieczeństwa infrastruktury serwerowej, w szczególności:
   a) analiza bezpieczeństwa zainstalowanych usług (czy zainstalowane oprogramowanie jest aktualne, czy zainstalowane oprogramowanie posiada znane luki w bezpieczeństwie, kto ma dostęp do udostępnionych usług),
   b) analiza bezpieczeństwa serwerów pod kątem dostępu użytkowników (czy jedynie uprawnieni użytkownicy mają dostęp do usług, czy udostępnione usługi zawierają jedynie te dane które są wymagane),
   c) analiza uprawnień poszczególnych użytkowników oraz grup użytkowników,

   d) analiza zbierania, przechowywania i monitorowania logów systemowych,
6. Weryfikacja bezpieczeństwa systemów (aplikacji), w których przetwarzane są dane osobowe.
7. Weryfikacja bezpieczeństwa stacji roboczych:
   a) analiza kontroli dostępu do stacji roboczych,
   b) analiza zainstalowanego oprogramowania znajdującego się na stacjach roboczych,
   c) analiza bezpieczeństwa stacji roboczych pod kątem zainstalowanych usług, dostępów zdalnych do stacji roboczych, bezpieczeństwa ochrony antywirusowej.
8. Weryfikacja zarządzania kopiami zapasowymi i ciągłością działania, w szczególności:
   a) analiza zakresu i częstotliwości wykonywania kopii zapasowych,
   b) analiza poprawności wykonywanych kopii zapasowych,
   c) analiza bezpieczeństwa przechowywania kopii zapasowych,
   d) analiza testów odtworzeniowych z kopii zapasowych,
   e) analiza procedur awaryjnych i planów ciągłości działania
   f) analiza niezawodności funkcjonowania systemów informatycznych
9. Przeprowadzenie nieinwazyjnych wewnętrznych i zewnętrznych testów penetracyjnych infrastruktury informatycznej.
10. Weryfikacja poprawności realizacji pozostałych obowiązków związanych z bezpieczeństwem systemów informatycznych, w szczególności w zakresie:
    a) zarządzania dostępem użytkowników do systemów informatycznych, w tym:
       – zasad rejestrowania użytkowników,
       – metod uwierzytelniania,
       – zasad nadawania i odbierania uprawnień,
       – przeglądów praw dostępu,
       – zarządzania kontami uprzywilejowanymi,
    b) instalacji i aktualizacji oprogramowania,
    c) ochrony przed szkodliwym oprogramowaniem,
    d) bezpieczeństwa pracy zdalnej,
    e) korzystania z urządzeń i nośników przenośnych,
    f) rozwoju systemów informatycznych,
    g) zarządzania zmianami w systemach informatycznych,
    h) przeglądów, konserwacji i napraw systemów informatycznych,
    i) rejestrowania działań administratorów i operatorów,
    j) zapisywania, przechowywania i monitorowania logów systemowych,
    k) synchronizacji zegarów,
    l) monitorowania bezpieczeństwa systemów informatycznych,
    m) monitorowania pojemności i wydajności systemów informatycznych,
    n) zapewnienia legalności oprogramowania,
    o) usuwania danych i niszczenia nośników danych,
    p) zarządzania incydentami bezpieczeństwa.

W czasie wykonania i po wykonaniu usługi infrastruktura Zamawiającego musi pozostać w niezmienionej formie, tj. nie może zostać uszkodzona, jak również nie mogą zostać usunięte, zmienione, nadpisane dane znajdujące się w tej infrastrukturze.

D. HARMONOGRAM REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1. Czynności audytowe w siedzibie Zamawiającego powinny odbyć się od 1.11.2022 r. do 08 12.2022 r.
2. W terminie do 7 dni od daty zakończenia audytu w siedzibie Zamawiającego, Wykonawca prześle raport wstępny.
3. Zamawiający ma prawo zgłoszenia uwag i zastrzeżeń do raportu wstępnego w ciągu 5 dni roboczych od jego otrzymania,
4. Wykonawca ustosunkuje się do zgłoszeni uwag w terminie 3 dni roboczych, w tym nanosząc ewentualne korekty do raportu wstępnego. W szczególnych przypadkach wymagających przeprowadzenia dodatkowych badań audytowych w celu wyjaśnienia zgłoszonych uwag lub zastrzeżeń, termin skorygowania raportu wstępnego może wydłużyć się o 5 dni roboczych.
5. Jeżeli Zamawiający nie będzie wnosił innych uwag lub zastrzeżeń do skorygowanego raportu wstępnego, poinformuje o tym Wykonawcę, który przygotuje na tej podstawie raport końcowy i przekaże go Zamawiającemu w terminie do 3 dni roboczych.
6. Raport końcowy odbioru przedmiotu zamówienia powinien być podpisany nie później niż 08.12.2022 r.

E. WARUNKI REALIZACJI AUDYTU

1. Zamawiający udostępni wszelkie niezbędne informacje oraz dyspozycyjność niezbędnych osób dla przeprowadzenia badań audytowych.
2. Zamawiający będzie udzielał odpowiedzi na wszelkie pytania audytowe oraz dostarczał wymagane dokumenty w ciągu 3 dni roboczych.
3. Zamawiający umożliwi zdalną realizację części badań audytowych pod warunkiem, że Wykonawca zapewni bezpieczeństwo dostępu zdalnego, oraz że badania będą się odbywały pod bieżącym nadzorem Zamawiającego.

F. INFRASTRUKTURA ZAMAWIAJĄCEGO

1. Liczba serwerów: do 40 w tym:
   – fizycznych: do 10

- wirtualnych: do 30

2. Liczba stanowisk komputerowych do 500
3. Ilość przełączników sieci komputerowych (głównych) – 2 szt.
4. Ilość przełączników dystrybucyjnych do 50
5. Systemy operacyjne serwerowe: Windows Serwer, Linux
6. Systemy operacyjne stacji roboczych. Windows 7, 8, 10
7. Ilość baz danych do 5
8. Liczba aplikacji bazodanowych – systemów przetwarzających dane i dane osobowe: do 20
9. Liczba serwerowni: 2
10. Liczba podsieci wewnętrznych LAN: do 5
11. Liczba punktów dostępowych Wi-Fi: do 100
12. Liczba urządzeń i systemów zapewniających dostęp do sieci Internet (serwerów brzegowych, urządzeń UTM, firewall, routerów, itp.): do 5
13. Liczba łącz internetowych: 3
14. Liczba publicznych adresów zewnętrznych: do 10
15. Active Directory: Wdrożona

G. DOKUMENTACJA

1. Wynikiem przeprowadzonych audytów i testów będzie raport zawierający:
   a) przedmiot, cel i zakres audytu,
   b) daty przeprowadzenia audytu,
   c) opis przyjętej metodyki,
   d) propozycje zmian w treści regulacji wewnętrznych dotyczących bezpieczeństwa informacji, w tym danych osobowych (dokumentacji SZBI) Zamawiającego,
   e) datę sporządzenia raportu,
   f) imiona i nazwiska audytorów realizujących zadanie oraz ich podpisy
   g) podsumowanie zarządcze (raport dla kierownictwa) obejmujące syntezę wyników audytu i ocenę poziomu spełnienia wymogów RODO, Rozporządzenia KRI, dokumentacji SZBI oraz ocenę bezpieczeństwa systemu informatycznego, w tym podsumowanie zidentyfikowanych słabości/nieprawidłowości, a także główne rekomendacje dotyczące poprawy bezpieczeństwa informacji, danych i systemu informatycznego,
   h) dokładny opis zidentyfikowanych nieprawidłowości, w szczególności:
      - wskazujący dokładne miejsca, w których występują realne bądź potencjalne problemy z bezpieczeństwem informacji,
      - zawierający wyniki audytów, w tym testów i ich interpretację – każde ustalenie musi odnosić się do konkretnych przypadków słabości/nieprawidłowości popartych zgromadzonymi dowodami audytowymi, które będą stanowiły załącznik do raportu,
      - zawierający rekomendacje w zakresie eliminacji zidentyfikowanych słabości/nieprawidłowości oraz poprawy poziomu bezpieczeństwa, w tym wskazanie działań korygujących i/lub doskonalących,
2. Ocena, ustalenia i rekomendacje muszą być ze sobą jasno powiązane i identyfikowalne.
3. Wszystkie wersje raportu wstępnego oraz raport końcowy zostaną przekazane w formie elektronicznej w formacie edytowalnym DOC oraz PDF. Pliki raportu zostaną zaszyfrowane programem 7-Zip przy użyciu algorytmu szyfrującego AES-256 oraz zabezpieczone co najmniej 12-znakowym hasłem (zawierającym małe i duże litery, cyfry i znaki specjalne) przesłanym przez alternatywny kanał komunikacji.
4. Wykonawca może dodatkowo przekazać raport końcowy, z wyłączeniem załączników zawierających dowody audytowe, w wersji wydruku w formacie A4.

H. WYMAGANIA

1. 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 w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wykaz certyfikatów wskazanych w w/w rozporządzeniu znajduje się poniżej:
   - Certified Internal Auditor (CIA),
   - Certified Information System Auditor (CISA),
   - 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,
   - 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,
   - Certified Information Security Manager (CISM),
   - Certified in Risk and Information Systems Control (CRISC),
   - Certified in the Governance of Enterprise IT (CGEIT),
   - Certified Information Systems Security Professional (CISSP),
   - Systems Security Certified Practitioner (SSCP),
   - Certified Reliability Professional,
   - Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.
2. Zamawiający wymaga dołączenia kopii certyfikatu osoby, która będzie przeprowadzała audyt do złożonej oferty.

3. Zamawiający wymaga, aby Wykonawca wykazał, że przeprowadził minimum 1 audyt cyberbezpieczeństwa w podmiocie publicznym w okresie ostatnich 3 lat.
4. Wykonawcy, którzy nie wykażą spełnienia warunków udziału w postępowaniu podlegać będą wykluczeniu. Ofertę Wykonawcy wykluczonego uznaje się za odrzuconą.