załącznik nr 2

**Opis przedmiotu zamówienia**

**„Przeprowadzenie audytu zgodności oraz świadczenie usług wsparcia merytorycznego w zakresie realizacji obowiązków Operatora Usług Kluczowych przez Szpital Specjalistyczny w Jaśle w ramach Krajowego Systemu Cyberbezpieczeństwa.”**

**I - Przedmiot zamówienia:**

Przeprowadzenie audytu zgodności oraz świadczenie usług wsparcia merytorycznego w zakresie realizacji obowiązków Operatora Usług Kluczowych przez Szpital Specjalistyczny w Jaśle w ramach Krajowego Systemu Cyberbezpieczeństwa.

Przedmiot Zamówienia zostanie wykonany w nawiązaniu do wymagań wynikających z:

Ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (UKSC), wdrażającej Dyrektywę NIS oraz Rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo,   
a także norm PN-ISO/IEC 27001, PN-EN/ISO 22301 oraz norm pokrewnych.

Na przedmiot zamówienia składa się:

1. Przeprowadzenia audytu zgodności (audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej) oraz opracowanie raportu z przeprowadzonego audytu w formie papierowej i elektronicznej;
2. Przeprowadzenia inwentaryzacji i klasyfikacji informacji;
3. Przeprowadzenia inwentaryzacji i klasyfikacji elementów składowych usługi kluczowej, w tym:
   1. zasobów informacyjnych,
   2. procesów i procedur,
   3. ról i uprawnień,
   4. kompetencji i kwalifikacji personelu,
   5. wsparcie w procesie inwentaryzacji sprzętu i oprogramowania;;
4. Przeprowadzenie analizy zagrożeń i oceny ryzyka systemów informacyjnych w nawiązaniu do przeprowadzonej klasyfikacji informacji;
5. Zaprojektowania, opracowania oraz dostosowania dokumentacji (polityki, regulaminy, procedury, rejestry, instrukcje itp.) w obszarze zarządzania bezpieczeństwem informacji (zgodnie z normą PN-ISO/IEC 27001, z uwzględnieniem norm: PN-EN ISO/IEC 27017, PN-EN ISO/IEC 27701, PN-EN ISO 27799),
6. Wsparcie przy zaprojektowaniu i doborze rozwiązań technicznych;
7. Szkolenia i warsztaty dla zespołu cyberbezpieczeństwa z zakresu realizacji obowiązków UKSC;
8. Świadczenie stałej usługi wsparcia merytorycznego wraz z nadzorem nad dokumentacją, w tym:
   1. konsultacje mailowe,
   2. konsultacje telefoniczne,
   3. konsultacje w siedzibie Zamawiającego,
   4. wizyty kontrolne w lokalizacjach Zamawiającego,
   5. nadzór nad systemem, z uwzględnieniem bieżącej aktualizacji dokumentacji w odnisieniu do prawnych i organizacyjnych,
   6. wsparcie obsługi incydentów;

**II - Wymagania:**

Przedmiot zamówienia może być wykonywany 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);

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.

**III - Termin realizacji zamówienia:**

Przedmiot zamówienia zostanie wykonany w terminie 12 miesięcy od podpisania umowy, przy czym audyt zgodności (audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej) oraz opracowanie raportu z przeprowadzonego audytu w formie papierowej i elektronicznej zostanie wykonany w ciągu 3 miesięcy od podpisania umowy.

**IV - Szczególne wymagania związane z przedmiotem zamówienia**

1. Zakres ogólny Dokumentacji KSC (pkt 5 OPZ), która zostanie opracowana i dostarczona, przy czym ostateczny zakres dostarczonej Dokumentacji KSC może, w wyniku uzgodnień stron umowy dotyczących prowadzonych ustaleń i prac projektowych, różnić się od przedstawionego poniżej i nie będzie stanowiło to zmiany warunków Umowy:
   1. Polityka Bezpieczeństwa Informacji (PBI);
   2. Polityka Bezpieczeństwa Danych Osobowych (PBDO) – wyłącznie weryfikacja zgodności i kompletności;
   3. Polityka Bezpieczeństwa Fizyczego i Środowiskowego (PBFiŚ) – wyłącznie weryfikacja zgodności i kompletności;
   4. Regulamin Bezpieczeństwa Teleinformatycznego (RBT);
   5. Metodyka Klasyfikacji Informacji i Analizy Ryzyk Bezpieczeństwa Informacji (MKIiARBI);
   6. Polityka Kontroli Dostępu (PKD);
   7. Procedura Audytu Wewnętrznego (PAW);
   8. Procedura Działań Korygujących i Zapobiegawczych SZBI (PDKiZ);
   9. Procedura Identyfikacji Wymagań (PIW);
   10. Procedura Nadzoru nad Dokumentacją i Zapisami SZBI (PNDiZ);
   11. Procedura Okresowych Przeglądów SZBI (POP);
   12. Procedura Przyjmowania Zgłoszeń oraz Podejmowania Działań Następczych (PPZoPDN);
   13. Procedura Rejestracji Korespondencji i Dokumentów (PRKiD);
   14. Procedura Zarządzania Incydentami Bezpieczeństwa Informacji (PZIBI);
   15. Procedura Zarządzania Uprawnieniami (PZU);
   16. Procedura Zgłaszania Incydentów (PZI);
   17. Procedura Logowania do Systemów (PLdS);
   18. Procedura dostępu do zasobów informatycznych (PDdZI);
   19. Procedura ustanawiania celów i pomiarów (PUCiP) – zasadność do ustalenia w toku prowadzonych prac realizacyjnych;
   20. Polityka Zabezpieczeń Kryptograficznych (PZK);
   21. Plan Postępowania z Ryzykiem (PPR);
   22. Plan Szkoleń i Uświadamiania (PSiU);
   23. Plan Ciągłości Działania (PCD) – wyłącznie weryfikacja zgodności i kompletności;
   24. Plan Odbudowy po Katastrofie (POpK) – wyłącznie weryfikacja zgodności i kompletności;
   25. Instrukcja komunikacji wewnętrznej i zewnętrznej – zasadność do ustalenia w toku prowadzonych prac realizacyjnych;
   26. Zakres i granice SZBI (ZiGS);
   27. Deklaracja Stosowania z wykazem niezbędnych zabezpieczeń i uzasadnieniem – zasadność do ustalenia w toku prowadzonych prac realizacyjnych;
   28. Procedura ustanawiania celów i pomiarów (PUCiP) – zasadność do ustalenia w toku prowadzonych prac realizacyjnych;
   29. Lista kontrolna aktywów – wyłącznie weryfikacja zgodności i kompletności;
   30. Zobowiązanie do zachowania poufności;
   31. Ocena Skutków Przetwarzania Danych – wyłącznie weryfikacja zgodności i kompletności;
   32. Regulamin Pracy Zdalnej (RPZ) – wyłącznie weryfikacja zgodności i kompletności;
2. Wymagania dotyczące stałej usługi wsparcia merytorycznego:
3. Czas reakcji na zgłoszony problem/pytanie merytoryczne z zakresu Systemu KSC nie przekroczy w ramach Dnia Roboczego:
   * 24 godzin w przypadku konsultacji mailowych,
   * 12 godzin w przypadku konsultacji telefonicznych;
4. Problemy/pytania powinny być zgłoszone:
   * pocztą elektroniczną na adres internetowy wskazany w Umowie przez Wykonawcę;
   * telefonicznie na numer telefonu komórkowego wskazany w Umowie przez Wykonawcę**;**

............................ ,dn. .............. ……....................................

*Podpis i pieczęć Wykonawcy*