Załącznik 1 do Zapytania o cenę

ZAMAWIAJĄCY:

BIURO RZECZNIKA PRAW PACJENTA
UL. PŁOCKA 11/13; 01-231 WARSZAWA

OPIS PRZEDMIOTU SZACOWANIA

WDROŻENIE I DOSKONALENIE SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W BIURZE RZECZNIKA PRAW PACJENTA WRAZ Z PRZEPROWADZENIEM AUDYTÓW WSTĘPNEGO I KOŃCOWEGO NA ZGODNOŚĆ Z ISO27001, KRI, UKSC.

PROJEKT
„CYBERBEZPIECZNY PACJENT”

1. PRZEDMIOT ZAMÓWIENIA

1.1. Zamówienie obejmuje świadczenie usług doradczych i wdrożeniowych polegających na przeprowadzeniu audytów systemów zarządzania bezpieczeństwem informacji przedwdrożeniowego i powdrożeniowego, opracowaniu, wdrożeniu, przeglądzie oraz aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) Zamawiającego.

1.2. Celem zamówienia jest osiągnięcie spójnego, udokumentowanego, działającego w praktyce SZBI, zapewniającego zarządzanie ryzykiem, zgodność prawną i organizacyjną oraz gotowość do audytów/kontroli (wewnętrznych i zewnętrznych) według najnowszych wymagań.

1.3. Przez pojęcie 'wdrożenie' Zamawiający rozumie realizację cyklu doskonalenia SZBI zgodnie z podejściem PDCA (plan–do–check–act), obejmującą audyt, analizę ryzyka, aktualizację dokumentacji oraz wdrożenie działań doskonalących.

1.4. Zamawiający posiada elementy SZBI, jednak nie posiada Systemu Zarządzania Bezpieczeństwem Informacji potwierdzonego jako zgodnego z wymaganiami w szczególności uKSC, KRI oraz normami serii ISO/IEC 27001 w najnowszych brzeminiach.

1.5. Zamówienie jest realizowane w reżimie grantu „Cyberbezpieczny Rząd", Wykonawca uwzględni wymagania sprawozdawcze, dowodowe i dokumentacyjne wynikające z zasad realizacji przedsięwzięcia oraz harmonogramu Zamawiającego.

1.6. Zamawiający przetwarza dane osobowe, w tym dane szczególnych kategorii (wrażliwe) dane medyczne. SZBI ma obejmować procesy i systemy związane z tym przetwarzaniem.

1.7. Środowisko teleinformatyczne Zamawiającego jest hybrydowe: Rozwiązania on-premises oraz usługi chmurowe.

1.8. Zamawiający wymaga, aby SZBI został opracowany i wdrożony co najmniej zgodnie z wymaganiami normy ISO/IEC 27001 (aktualne wydanie) oraz z uwzględnieniem ISO/IEC 27002 jako katalogu środków bezpieczeństwa – albo Rozwiązania równoważnego. Przez „równoważność" rozumie się spełnienie celów i zakresu wymagań normy (w szczególności: podejście oparte o ryzyko, cykl PDCA / ciągłe doskonalenie, udokumentowane procesy i dowody ich działania) przy zachowaniu porównywalnego poziomu dojrzałości i kompletności.

1.9. Opracowany i wdrożony SZBI musi być w pełni zgodny z wymaganiami następujących dokumentów (w ich najnowszych, obowiązujących na dzień udzielenia zamówienia wersjach):

1.9.1. Norma ISO/IEC 27001 - "Information security, cybersecurity and privacy protection — Information security management systems — Requirements".

1.9.2. Norma ISO/IEC 27005 - "Information security, cybersecurity and privacy protection — Guidance on managing information security risks".

1.9.3. Norma PN-ISO/IEC 29134 – Wytyczne do przeprowadzenia oceny skutków dla prywatności (DPIA)

1.10. Wykonawca zapewni zgodność SZBI co najmniej z wymaganiami wynikającymi z właściwych przepisów dla Zamawiającego, w tym w szczególności:

1.10.1. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, „RODO”),

1.10.2. Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2023 poz. 913 ze zm.) wraz z aktami wykonawczymi do tej ustawy („uKSC”),

1.10.3. rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (KRI) oraz minimalnych wymagań dla systemów teleinformatycznych

1.10.4. Ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz.U. z 2023 r. poz. 1270 ze zm.);

1.11. W przypadku, gdy w trakcie realizacji zamówienia ww. akty prawne ulegną zmianie Wykonawca powinien przedstawić Zamawiającemu zakres niezbędnych zmian w zakresie aktualizacji przygotowanego SZBI

2. ETAP 1 AUDYT SZBI

2.1. W ramach zadania Wykonawca zapewni przeprowadzenie szczegółowego audytu przedwdrożeniowego istniejącej dokumentacji Zamawiającego, realizowanego przez wykwalifikowanego, zewnętrznego audytora.

2.2. Celem audytu jest identyfikacja luk w obecnym stanie SZBI, weryfikacja zgodności z wymaganiami oraz ocena poziomu dojrzałości procesów bezpieczeństwa.

2.3. Audyt obejmie działalność Zamawiającego w zakresie niezbędnym do potwierdzenia zgodności wdrożonych rozwiązań i praktyk z:

2.3.1. normą ISO/IEC 27001 (oraz powiązanymi normami z rodziny ISO/IEC 27000 – w zakresie wspierającym ocenę zgodności),

2.3.2. rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (KRI) oraz minimalnych wymagań dla systemów teleinformatycznych,

2.3.3. ustawą o krajowym systemie cyberbezpieczeństwa (uKSC).

2.4. Audyt obejmie co najmniej:

2.4.1. identyfikację procesów biznesowych istotnych dla bezpieczeństwa informacji,
2.4.2. identyfikację i inwentaryzację aktywów informacyjnych, technicznych oraz organizacyjnych (w zakresie niezbędnym do oceny zgodności),
2.4.3. analizę kontekstu organizacji, w tym identyfikację interesariuszy oraz ich wymagań,
2.4.4. przegląd i ocenę dokumentacji wewnętrznej Zamawiającego (regulaminy, procedury, instrukcje oraz inne akty wewnętrzne) pod kątem wpływu na bezpieczeństwo informacji i zgodność z ww. wymaganiami,
2.4.5. weryfikację spełnienia wymagań oraz identyfikację braków, niezgodności i obszarów do doskonalenia.
2.5. W analizie stanu obecnego Wykonawca uwzględni obowiązujące u Zamawiającego wewnętrzne akty prawa. Zamawiający udostępni je do wglądu.
2.6. Audyt musi zostać wykonany przez niezależnych audytorów posiadających ważny certyfikat audytora wiodącego ISO/IEC 27001.
2.7. Wykonawca przedstawi wyniki audytu w sposób umożliwiający jednoznaczne określenie poziomu zgodności Zamawiającego z wymaganiami, w tym co najmniej:
2.7.1. opis zakresu, metodyki oraz zastosowanych technik audytowych,
2.7.2. ocenę stanu SZBI i dojrzałości procesów bezpieczeństwa,
2.7.3. zestawienie ustaleń audytowych wraz z odniesieniem do konkretnych wymagań ISO/IEC 27001, KRI i uKSC (wskazanie punktu/artykułu/paragrafu),
2.7.4. wskazanie obszarów wymagających poprawy oraz dobrych praktyk zaobserwowanych u Zamawiającego.
2.8. W ramach realizacji zamówienia Wykonawca dostarczy:
2.8.1. raport audytowy z oceny zgodności z ISO/IEC 27001, KRI, uKSC,
2.8.2. prezentację podsumowującą wyniki audytu dla kierownictwa Zamawiającego.
2.9. Wykonawca opracuje i dostarczy wykaz niezgodności, obserwacji oraz rekomendacji, obejmujący co najmniej:
2.9.1. identyfikator ustalenia,
2.9.2. klasyfikację (np. niezgodność / obserwacja / rekomendacja), poziom istotności,
2.9.3. odniesienie do wymagania (ISO/IEC 27001 / KRI / uKSC – z podaniem właściwego punktu/artykułu/paragrafu),
2.9.4. opis stanu faktycznego i wskazanie dowodów audytowych (w zakresie dopuszczalnym),
2.9.5. opis ryzyka/konsekwencji,
2.9.6. rekomendowany kierunek działań korygujących lub doskonalących.

2.10. Wykonawca opracuje i dostarczy wykaz działań niezbędnych do osiągnięcia pełnej zgodności, co najmniej w postaci planu działań korygujących i doskonalących, zawierającego dla każdego ustalenia:
2.11. proponowane działanie,
2.12. priorytet i kolejność realizacji (zależności),
2.13. harmonogram działań Wykonawcy,
2.14. właściciela działania po stronie Zamawiającego (rola/komórka),
2.15. wymagane zasoby (opisowo),
2.16. rekomendowany termin realizacji.
2.17. W analizie staniu obecnego Wykonawca weźmie pod uwagę obowiązujące u Zamawiającego wewnętrzne akty prawa. Zamawiający udostępni do wglądu treści ww. dokumentów.

3. ETAP 2 SZACOWANIE I ANALIZA RYZYKA

3.1. Wykonawca opracuje powszechnie uznaną i zaakceptowaną przez Zamawiającego metodykę analizy ryzyka zgodnej z normą ISO/IEC 27005.
3.2. Wykonawca przeprowadzi analizę ryzyka bezpieczeństwa informacji, obejmującą co najmniej:
3.2.1. identyfikację zagrożeń i podatności;
3.2.2. ocenę skutków i prawdopodobieństwa wystąpienia ryzyk;
3.2.3. określenie poziomu ryzyka oraz sposobów jego postępowania (akceptacja, redukcja, transfer, unikanie).
3.2.4. Wykonawca opracuje i przekaże Zamawiającemu kompletną dokumentację z analizy ryzyka zawierającą:
3.2.5. Rejestr Aktywów Informacyjnych.
3.2.6. Raport z Analizy Ryzyka zawierający zidentyfikowane ryzyka wraz z ich oceną.
3.2.7. Plan Postępowania z Ryzykiem, określający sposób reakcji na każde zidentyfikowane ryzyko (akceptacja, mitygacja, transfer, unikanie).
3.3. Wykonawca zobowiązany jest uwzględnić w planowanym szacowaniu, analizie i postępowaniu z ryzkami w zakresie bezpieczeństwa informacji, również specyfikę bezpieczeństwa danych osobowych i specyfikę organu publicznego.
3.4. Metodyka analizy ryzyka zgodna z normą ISO/IEC 27005, winna obejmować również kryterium ryzyka w oparciu o przepisy RODO. W tym przypadku winny być uwzględnione ryzyka dla praw i wolności osób fizycznych, a następnie zaproponowanie w uzgodnieniu z Administratorem odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych osobowych.
3.5. Wykonawca zapewni spójność produktów etapu z dokumentacją dotyczącą Kontroli Zarządczej obowiązującej u Zamawiającego.

4. ETAP 3 WDROŻENIE I DOSKONALENIE SZBI

4.1. Wykonawca dokona przeglądu, aktualizacji, dostosowania oraz uzupełnienia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji Zamawiającego, zgodnie z normami serii ISO/IEC 27001, KRI oraz uKSC w ich najnowszych wersjach, w oparciu o wyniki audytu oraz analizy ryzyka.

4.2. Wykonawca opracuje zaktualizowany kompletny zestaw dokumentacji SZBI zgodniej z normami serii 27001, KRI i UKSC w najnowszych wersjach, poprzez dostosowanie istniejącej dokumentacji Zamawiającego oraz utworzenie nowej, jeśli jest wymagana.

4.3. Wszystkie dokumenty muszą być opracowane w ścisłej współpracy z Zamawiającym i w pełni dostosowane do specyfiki jego działalności, procesów, zasobów oraz infrastruktury.

4.4. Niedopuszczalne jest dostarczenie generycznych, niezaadaptowanych szablonów.

4.5. Akceptacja dokumentacji będzie uzależniona od wykazania, że odnosi się ona do realnych, nazwanych procesów, zasobów i ról funkcjonujących u Zamawiającego.

4.6. Minimalny zakres dokumentacji obejmuje aktualizację, uzupełnienie lub – w uzasadnionych przypadkach – opracowanie brakujących dokumentów, w szczególności:

4.6.1. Księga SZBI (podręcznik systemu).

4.6.2. Polityka Bezpieczeństwa Informacji.

4.6.3. Deklaracja Stosowania (SoA).

4.6.4. Aktualizację Polityki Ochrony Danych Osobowych (zgodna z RODO).

4.6.5. Polityki szczegółowe, zasady i procedury wynikające z aktów normatywnych w szczególności:

4.6.6. Zarządzanie aktywami.

4.6.7. Bezpieczeństwo osobowe (cykl życia pracownika).

4.6.8. Zarządzanie uprawnieniami i dostępem.

4.6.9. Bezpieczeństwo fizyczne i środowiskowe.

4.6.10. Bezpieczeństwo teleinformatyczne (sieci, systemy, aplikacje).

4.6.11. Zarządzanie incydentami bezpieczeństwa informacji.

4.6.12. Zarządzanie ciągłością działania.

4.6.13. Zasady zgodności z wymaganiami prawnymi i umownymi.

4.6.14. Wzory rejestrów

4.6.15. Polityka klasyfikacji informacji,

4.6.16. Polityka zarządzania dostępem i uprawnieniami,

4.6.17. Polityka zarządzania podatnościami,

4.6.18. Polityka zarządzania ryzykiem z uwzględnieniem obszaru cyberbezpieczeństwa i przetwarzania danych osobowych,

4.6.19. Polityka zarządzania incydentami cyberbezpieczeństwa i danych osobowych,
4.6.20. Polityka zarządzania ciągłością działania z uwzględnieniem Planu Ciągłości Działania (BCP) oraz Plan Odzyskiwania po Awarii (Disaster Recovery Plan - DRP),
4.6.21. Polityka logowania zdarzeń z uwzględnieniem aplikacji, sieci, serwerów, bramy brzegowej, kontrolera domeny,
4.6.22. Procedura zarządzania dostawcami (zarządzania łańcuchem dostaw),
4.6.23. Procedura zarządzania zmianami w urządzeniach i systemach IT,
4.6.24. Procedura zarzadzania pojemnością i wydajnością krytycznych zasobów teleinformatycznych,
4.6.25. Procedura zarządzania dokumentacja i zapisami SZBI,
4.6.26. Procedura audytów wewnętrznych SZBI.
4.6.27. Inne dokumenty (instrukcje, regulaminy, wzory oświadczeń), których potrzeba opracowania zostanie zidentyfikowana i uzasadniona w tym wymagana przez normy serii 27001.
4.7. Kompletna, zatwierdzona przez Zamawiającego dokumentacja SZBI musi być dostarczona w edytowalnej formie elektronicznej (np. format .docx).
4.8. Zamawiający informuje, że posiada opracowany dokument Polityki Ochrony Danych Osobowych. Wykonawca zobowiązany jest uwzględnić zapisy tego dokumentu w przygotowanym SZBI i przygotować SZBI w taki sposób, aby zapisy Systemu były spójne z ww. dokumentem.
4.9. Wykonawca jest zobowiązany do prowadzenia prac w taki sposób, aby zapewnić personelowi Zamawiającego transfer wiedzy umożliwiający samodzielne utrzymanie i doskonalenie SZBI po zakończeniu umowy.
4.10. Zamawiający zobowiązuje się do aktywnej współpracy z Wykonawcą, w tym do zapewnienia dostępu do niezbędnej dokumentacji, personelu oraz pomieszczeń w uzgodnionych terminach.
4.11. Wykonawca zobowiązany jest do realizacji zamówienia zgodnie z zasadą "nie czyń poważnych szkód" (DNSH - Do No Significant Harm), co oznacza, że wdrożone Rozwiązania nie mogą wywierać negatywnego wpływu na cele środowiskowe.
4.12. Odbiór każdego etapu będzie następował na podstawie protokołu zdawczo-odbiorczego, podpisanego bez uwag przez obie strony, po weryfikacji kompletności i jakości dostarczonych produktów.
4.13. Zamawiający ma 10 dni roboczych na zgłoszenie uwag do przekazanych materiałów, które Wykonawca musi uwzględnić w dalszych działaniach.
4.14. Wszystkie produkty cyfrowe (w tym m.in. raporty, polityki, procedury, materiały szkoleniowe) wytworzone przez Wykonawcę w ramach realizacji zamówienia muszą spełniać standardy dostępności cyfrowej

określone w dokumencie "Standardy dostępności dla polityki spójności 2021-2027".

4.15. Wykonawca zapewni, że zakres prac dokumentacyjnych nie będzie prowadził do dublowania istniejących efektów, a każda zmiana, aktualizacja lub nowy dokument będzie posiadał uzasadnienie wynikające z audytu, analizy ryzyka lub zmiany przepisów/norm.

5. ETAP 4 SZKOLENIA Z SZBI

5.1. Przedmiotem zadania jest przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa dla kadry Zamawiającego, istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji oraz SZBI.

5.2. Celem szkolenia jest zapewnienie, że kadra w tym osoby pełniące kluczowe funkcje rozumieją swoje role i odpowiedzialności w zakresie cyberbezpieczeństwa oraz potrafią podejmować decyzje zgodne z polityką bezpieczeństwa informacji i SZBI.

5.3. Szkolenie musi mieć charakter strategiczno-decyzyjny, łączący elementy teoretyczne z analizą przypadków, scenariuszy decyzyjnych oraz dyskusją moderowaną.

5.4. Wykonawca jest zobowiązany do prowadzenia prac w taki sposób, aby zapewnić personelowi Zamawiającego transfer wiedzy umożliwiający samodzielne utrzymanie i doskonalenie SZBI po zakończeniu umowy.

5.5. Liczba uczestników zostanie określona przez Zamawiającego na etapie realizacji umowy.

5.6. Szkolenie może być realizowane w formie stacjonarnej lub hybrydowej, w siedzibie Zamawiającego lub innym wskazanym miejscu na terenie miasta stołecznego Warszawy.

5.7. Minimalny czas trwania szkolenia wynosi 1 dzień szkoleniowy (co najmniej 6–8 godzin zegarowych).

5.8. Liczba osób do przeszkolenia ok. 130 przy czym maksymalna grupa szkoleniowa może wynosić 50 osób.

5.9. Szkolenie musi być bezpośrednio powiązane z funkcjonującym lub wdrażanym SZBI Zamawiającego, w tym z polityką bezpieczeństwa informacji oraz procedurami bezpieczeństwa.

5.10. Wykonawca omówi rolę kadry w systemie zarządzania bezpieczeństwem informacji, odpowiedzialności zarządczej oraz wpływu decyzji kierowniczych na poziom bezpieczeństwa.

6. USŁUGA UTRZYMANIA I DOSKONALENIA SZBI

6.1. Przedmiotem zadania jest świadczenie usługi utrzymania oraz doskonalenia (rozwoju) SZBI u Zamawiającego, w okresie **36 miesięcy od dnia zawarcia umowy**.

6.2. Usługa świadczona jest wyłącznie na podstawie zleceń (zamówień) składanych przez Zamawiającego, rozliczanych według liczby faktycznie wykonanych i odebranych godzin. Zamawiający nie gwarantuje minimalnej liczby godzin.

6.3. Łączny limit prac w ramach umowy wynosi do **200 godzin**. Po wykorzystaniu limitu dalsze prace wymagają odrębnego zamówienia/umowy.

6.4. Usługa obejmuje bieżące utrzymanie SZBI:

6.4.1. Utrzymanie aktualności i spójności dokumentacji SZBI, w tym polityk, procedur, instrukcji i rejestrów.

6.4.2. Aktualizacje dokumentacji wynikające ze zmian u Zamawiającego (organizacyjnych, procesowych, technicznych) – w części dokumentacyjnej.

6.4.3. Prowadzenie wersjonowania, rejestru zmian i porządkowanie dokumentów (nadzór nad dokumentacją).

6.4.4. Utrzymanie matrycy zgodności / mapowania do ISO/IEC 27001, KRI i uKSC (w zakresie dokumentacyjnym).

6.4.5. Wsparcie w obsłudze niezgodności i działań korygujących od strony formalnej (zapisy, rejestry, aktualizacje dokumentów).

6.5. Prace realizowane będą zdalnie, a jeśli Zamawiający tego wymaga – również w trybie w siedzibie Zamawiającego) w uzgodnionych terminach.

7. AUDYT KOŃCOWY SZBI

7.1. Kryterium odbioru ETAPU 2 i 3 stanowi przedstawienie przez Wykonawcę raportu z audytu przeprowadzonego przez audytorów niezależnych od Wykonawcy, posiadających ważne uprawnienia/audytorskie kwalifikacje w zakresie SZBI, potwierdzającego spełnienie wymagań:

7.1.1. ISO/IEC 27001 (oraz powiązanych wymagań z rodziny ISO/IEC 27000 w zakresie mającym zastosowanie),

7.1.2. KRI

7.1.3. uKSC,

7.1.4. Audyt nie może stwierdzać niezgodności krytycznych uniemożliwiających uznanie SZBI za zgodny w wymaganiami.

7.2. W przypadku stwierdzenia niezgodności niekrytycznych, odbiór może nastąpić po przedstawieniu i akceptacji planu działań korygujących oraz usunięciu niezgodności w terminie uzgodnionym z Zamawiającym.