

Załącznik nr 1 do zapytania ofertowego nr KPOC/4/2025 – Szczegółowy opis przedmiotu zamówienia (SOPZ)**Załącznik nr 1 do Oferty**

LUX MED Onkologia sp. z o.o.
ul. Szamocka 6, 01-748 Warszawa

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiot zamówienia – przeprowadzenie niezależnego audytu końcowego w obszarze cyberbezpieczeństwa, potwierdzającego zabezpieczenie przetwarzania elektronicznej dokumentacji medycznej (EDM), zgodnie z wymaganiami inwestycji D.1.1.2 KPO oraz kryteriami akceptacji do oceny przy audycie końcowym.

Audyt musi umożliwić Zamawiającemu wykazanie realizacji wskaźnika D21G.R2 – „Zabezpieczenie przetwarzania elektronicznej dokumentacji medycznej potwierdzone audytem bezpieczeństwa”.

Opis kolumn tabeli – Instrukcja dla Wykonawcy

Poniższa tabela zawiera minimalne wymagania dotyczące realizacji usługi audytu końcowego w obszarze cyberbezpieczeństwa oraz wymagane informacje identyfikujące sposób realizacji audytu, które muszą zostać spełnione i podane przez Wykonawcę.

1. Lp.

Numer porządkowy parametru.

2. PARAMETRY WYMAGANE

Określa minimalne wymagania dotyczące realizacji usługi audytu końcowego w obszarze cyberbezpieczeństwa, w tym: zakres audytu, sposób realizacji oraz wymagane produkty końcowe audytu

3. WARTOŚĆ WYMAGANA

Określa sposób potwierdzenia spełnienia danego parametru:

- TAK – parametr obowiązkowy (minimalny), wymagany do spełnienia.
- TAK, podać ... – parametr obowiązkowy (minimalny), wymagany do spełnienia i opisanie wartości.
- TAK, podać \geq ... / \leq ... / $>$... / $<$... / $=$... – parametr obowiązkowy (minimalny), dla którego należy spełnić określony próg wartości. Jeżeli jednocześnie w kolumnie ZASADY PRYZNAWANIA PUNKTÓW / INFORMACJA O PUNKTACJI wskazano możliwe do uzyskania punkty – oznacza to, że podana minimalna/maksymalna wartość musi zostać spełniona. Brak spełnienia tej wartości skutkuje odrzuceniem oferty. W przypadku parametrów punktowanych, spełnienie wartości ponad minimalną lub poniżej maksymalnej w określonym zakresie może wpływać na przyznanie punktów (zgodnie z kolumną ZASADY PRYZNAWANIA PUNKTÓW / INFORMACJA O PUNKTACJI).
- TAK / NIE (podać) — parametr fakultatywny (nieobowiązkowy); Wykonawca może, ale nie musi go spełniać. Za spełnienie tego wymogu Wykonawca otrzyma punkty zgodnie z wartościami w kolumnie ZASADY PRYZNAWANIA PUNKTÓW / INFORMACJA O PUNKTACJI. Brak spełnienia tego parametru lub wpisanie słowa „NIE”, lub pozostawienie pustego pola spowoduje nieprzyznanie punktów, ale nie skutkuje odrzuceniem oferty.

Wykonawca w kolumnie MIEJSCE NA INFORMACJE WYKONAWCY wskazuje oferowaną wartość danego parametru, zgodnie z zasadami opisanymi powyżej. Wskazanie wartości odpowiednio wyższej lub niższej niż minimalna/maksymalna powoduje przyznanie punktów zgodnie z wartościami wskazanymi w kolumnie ZASADY PRYZNAWANIA PUNKTÓW / INFORMACJA O PUNKTACJI. Spełnienie minimalnego/maksymalnego progu jest warunkiem dopuszczenia oferty. Jeżeli parametr jest punktowany, Wykonawca może uzyskać punkty odpowiednio do zadeklarowanej wartości. Niespełnienie minimalnego/maksymalnego progu skutkuje odrzuceniem oferty.

UWAGA: Wykonawca zobowiązany jest do podania wartości parametrów w jednostkach wskazanych w opisie danego parametru.

4. MIEJSCE NA INFORMACJE WYKONAWCY

Wykonawca zobowiązany jest wpisać w tej kolumnie:

- TAK – dla potwierdzenia spełnienia parametru obowiązkowego lub podania wymaganej informacji identyfikacyjnej.
- TAK oraz podać wartość/dane/opis – jeżeli w kolumnie „WARTOŚĆ WYMAGANA” wskazano „podać” (np. metodyka audytu, skład zespołu, termin realizacji, format raportu).
- TAK / NIE oraz podać wartość/dane/opis – w przypadku parametrów fakultatywnych (jeżeli występują).

Pozostawienie pustego pola lub wpisanie „NIE” dla parametrów obowiązkowych skutkuje odrzuceniem oferty.

Brak wpisu lub wpisanie „NIE” dla parametrów fakultatywnych spowoduje nieprzyznanie punktów (jeżeli przewidziano punktację), ale nie spowoduje odrzucenia oferty.

5. ZASADY PRYZNAWANIA PUNKTÓW / INFORMACJA O PUNKTACJI

Kolumna zawiera informację dla Wykonawcy, czy za dany parametr przyznawane są punkty w ramach kryteriów oceny ofert, a jeżeli tak – w jaki sposób.

- Dla parametrów niepunktowanych – w tej kolumnie znajduje się informacja „nie dotyczy (N/D)” lub „bez punktacji”.
- Dla parametrów punktowanych – w tej kolumnie podane są zasady przyznawania punktów.

Uwaga: Ocena oferty następuje na podstawie informacji podanych przez Wykonawcę w kolumnie MIEJSCE NA INFORMACJE WYKONAWCY, przy uwzględnieniu zasad wskazanych w niniejszej kolumnie oraz w zapytaniu ofertowym.

W przypadku wątpliwości, czy oferowany parametr jest spełniony, Zamawiający może zażądać od Wykonawcy dokumentów/wyjaśnień potwierdzających spełnienie wymagań SOPZ; niewykazanie spełnienia wymagań na żądanie Zamawiającego skutkować będzie odrzuceniem oferty.

	PARAMETRY WYMAGANE	WARTOŚĆ WYMAGANA	MIEJSCE NA INFORMACJE WYKONAWCY (wpisać "TAK" jeżeli oferta spełnia dany parametr, a także wpisać dodatkowe informacje, o ile z opisu w kolumnie "PARAMETRY WYMAGANE" wynika taki obowiązek)	ZASADY PRYZNAWANIA PUNKTÓW / INFORMACJA O PUNKTACJI
I.	System kopii zapasowych			N/D
1.	Audyt weryfikuje objęcie backupem wszystkich kluczowych i pomocniczych systemów objętych systemem kopii zapasowych	TAK		<i>bez punktacji</i>
2.	Audyt weryfikuje dokumentację dotyczącą częstotliwości wykonywania kopii zapasowych	TAK		<i>bez punktacji</i>
3.	Audyt weryfikuje dokumentację procedur wykonywania i odtwarzania kopii	TAK		<i>bez punktacji</i>
4.	Audyt weryfikuje procedury odmiejszczenia kopii	TAK		<i>bez punktacji</i>
5.	Audyt weryfikuje procedury testów odtworzeniowych	TAK		<i>bez punktacji</i>
6.	Audyt weryfikuje raporty z wykonywania backupów	TAK		<i>bez punktacji</i>
7.	Audyt weryfikuje zarządzanie dostępem do systemu backupu	TAK		<i>bez punktacji</i>
8.	Audyt weryfikuje wyniki testów funkcjonalnych i niefunkcjonalnych działania systemu backup	TAK		<i>bez punktacji</i>
9.	Audyt weryfikuje zgodność konfiguracji z dokumentacją	TAK		<i>bez punktacji</i>
10.	Audyt weryfikuje potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi systemu kopii zapasowej	TAK		<i>bez punktacji</i>
II.	Zapory sieciowe			
11.	Audyt weryfikuje dokumentację powykonawczą wdrożonych zapór sieciowych wraz z zabezpieczeniami	TAK		<i>bez punktacji</i>
12.	Audyt weryfikuje testy skuteczności zabezpieczeń	TAK		<i>bez punktacji</i>

13.	Audyt weryfikuje zgodność konfiguracji z dokumentacją	TAK		<i>bez punktacji</i>
14.	Audyt obejmuje analizę konfiguracji urządzeń oraz testy kontrolne poprawności działania zabezpieczeń.	TAK		<i>bez punktacji</i>
III.	Ochrona poczty e-mail			
15.	Audyt weryfikuje sposób ochrony poczty wraz z dokumentacją systemów ochrony poczty	TAK		<i>bez punktacji</i>
16.	Audyt weryfikuje wdrożenie polityk ochrony poczty w tym SPF, DKIM, DMARC).	TAK		<i>bez punktacji</i>
17.	Audyt weryfikuje wdrożenie 2FA dla dostępu publicznego	TAK		<i>bez punktacji</i>
18.	Audyt weryfikuje backup poczty i test odtworzeniowy	TAK		<i>bez punktacji</i>
19.	Audyt weryfikuje aktualizacje systemu	TAK		<i>bez punktacji</i>
20.	Audyt weryfikuje test poprawności konfiguracji (np. z wykorzystaniem narzędzi CERT Polska)	TAK		<i>bez punktacji</i>
21.	Audyt weryfikuje politykę bezpiecznego korzystania z poczty	TAK		<i>bez punktacji</i>
IV.	Segmentacja sieci			
22.	Audyt weryfikuje podział sieci wraz ze sposobem implementacji	TAK		<i>bez punktacji</i>
23.	Audyt weryfikuje sposób identyfikowania, uwierzytelniania i autoryzacji urządzeń podłączanych do sieci	TAK		<i>bez punktacji</i>
24.	Audyt weryfikuje zgodność konfiguracji z dokumentacją	TAK		<i>bez punktacji</i>
25.	Audyt potwierdza uczestnictwo na szkoleniach z zakresu obsługi zainstalowanych systemów ochrony sieciowej	TAK		<i>bez punktacji</i>
26.	Weryfikację potwierdzającą skuteczność wprowadzonych zabezpieczeń	TAK		<i>Bez punktacji</i>

V.	Ochrona stacji roboczych oraz serwerów (rozwiązania klasy EDR)			
27.	Audyt weryfikuje dokumentację powykonawczą wdrożonego rozwiązania, potwierdzającą zastosowanie polityk bezpieczeństwa oraz wdrożenie agentów rozwiązania na stacjach roboczych oraz serwerach	TAK		<i>bez punktacji</i>
28.	Audyt potwierdza uczestnictwo na szkoleniach z zakresu obsługi zainstalowanych systemów ochrony sieciowej	TAK		<i>bez punktacji</i>
VI.	Zarządzanie podatnościami			
29.	Audyt weryfikuje wdrożenie systemu automatycznego skanowania podatności (sieciowego i/lub agentowego).	TAK		<i>bez punktacji</i>
30.	Audyt weryfikuje warunki świadczenia wsparcia (SLA/terminy napraw).	TAK		<i>bez punktacji</i>
VII.	System zarządzania bezpieczeństwem informacji			
31.	Audyt weryfikuje ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)	TAK		<i>bez punktacji</i>
32.	Audyt weryfikuje polityki bezpieczeństwa (m.in. dostęp, kryptografia, backup, incydenty, ciągłość działania)	TAK		<i>bez punktacji</i>
33.	Audyt weryfikuje dokumentację	TAK		<i>bez punktacji</i>
34.	Audyt potwierdza alokację zasobów	TAK		<i>bez punktacji</i>
35.	Audyt ocenia funkcjonowanie systemów w praktyce	TAK		<i>bez punktacji</i>
36.	Audyt potwierdza uczestnictwo na szkoleniach.	TAK		<i>bez punktacji</i>
VIII.	Szkolenia z zakresu cyberbezpieczeństwa			
37.	Audyt weryfikuje programy szkoleń	TAK		<i>bez punktacji</i>
38.	Audyt weryfikuje potwierdzenia udziału min. 75% pracowników kadry medycznej i biurowej	TAK		<i>bez punktacji</i>
39.	Audyt weryfikuje potwierdzenia udziału min. 75% kadry kierowniczej	TAK		<i>bez punktacji</i>

40.	Audyt weryfikuje zakres merytoryczny zgodny z wymaganiami KPO	TAK		<i>bez punktacji</i>
IX.	Usługi zarządzane bezpieczeństwem			
41.	Audyt weryfikuje funkcjonowanie monitoringu 24/7	TAK		<i>bez punktacji</i>
42.	Audyt weryfikuje dokumentację scenariuszy reakcji.	TAK		<i>bez punktacji</i>
43.	Audyt weryfikuje funkcjonowanie systemu SIEM	TAK		<i>bez punktacji</i>
44.	Audyt weryfikuje raporty dzienne/miesięczne	TAK		<i>bez punktacji</i>
X.	Uwierzytelnianie i autoryzacja			
45.	Audyt weryfikuje wdrożenie MFA dla systemów krytycznych	TAK		<i>bez punktacji</i>
46.	Audyt weryfikuje wdrożenie 2FA lub bezhasłowe uwierzytelnianie dla użytkowników (zgodnie z przyjętą polityką)	TAK		<i>bez punktacji</i>
47.	Audyt weryfikuje obecność 2FA dla VPN	TAK		<i>bez punktacji</i>
48.	Audyt weryfikuje eliminację SMS jako drugiego składnika	TAK		<i>bez punktacji</i>
49.	Audyt weryfikuje zgodność ze standardem FIDO2	TAK		<i>bez punktacji</i>
50.	Audyt weryfikuje dokumentację powykonawczą	TAK		<i>bez punktacji</i>
51.	Audyt weryfikuje testy poprawności konfiguracji	TAK		<i>bez punktacji</i>
XI.	Raport końcowy z audytu			
52.	Raport będzie zawierał opis zakresu i dat realizacji audytu	TAK		<i>bez punktacji</i>
53.	Raport będzie zawierał opis metodyki	TAK		<i>bez punktacji</i>
54.	Raport będzie zawierał wykaz systemów i obszarów objętych audytem	TAK		<i>bez punktacji</i>
55.	Raport będzie zawierał ocenę spełnienia kryteriów obligatoryjnych i nieobligatoryjnych	TAK		<i>bez punktacji</i>

56.	Raport będzie zawierał matrycę wyników (obszar, obligatoryjność, wynik, dowód, uwagi)	TAK		<i>bez punktacji</i>
57.	Raport będzie zawierał klasyfikację niezgodności (krytyczna/istotna/drobna)	TAK		<i>bez punktacji</i>
58.	Raport będzie zawierał rekomendacje działań naprawczych	TAK		<i>bez punktacji</i>
59.	Raport będzie zawierał jednoznaczną opinię końcową (pozytywną albo warunkowo pozytywną)	TAK		<i>bez punktacji</i>
60.	Raport końcowy będzie dostarczony w formie elektronicznej, w formatach otwartych (PDF, DOCX, XLSX, XML, CSV, PNG, SVG, lub równoważnych), umożliwiającym jego odczytywanie i aktualizację bez stosowania narzędzi licencjonowanych	TAK		<i>bez punktacji</i>
61.	Raport będzie zawierał listę załączników	TAK		<i>bez punktacji</i>
62.	Raport będzie zawierał podpisy audytorów	TAK		<i>bez punktacji</i>

.....
(data i podpis osoby uprawnionej do złożenia Oferty w imieniu Wykonawcy)