OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Audyt spełnienia obligatoryjnych kryteriów ankiety dojrzałości cyberbezpieczeństwa oraz szkolenia z zakresu cyberbezpieczeństwa

w ramach projektu cyfryzacji podmiotu leczniczego - zadanie D 1.1.2

1. Kontekst zamówienia

Zamówienie realizowane jest w ramach projektu cyfryzacji podmiotu leczniczego, którego celem jest rozwój e-usług, digitalizacja dokumentacji medycznej, rozwój systemów informatycznych oraz zwiększenie poziomu cyberbezpieczeństwa przetwarzania danych medycznych i danych osobowych.

Przedmiot zamówienia obejmuje usługę audytu cyberbezpieczeństwa, przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa Audyt ma potwierdzić spełnienie wymagań obligatoryjnych ankiety, a działania proceduralne mają ujednolicić sposób wytwarzania, obiegu, zatwierdzania, archiwizacji i udostępniania dokumentacji EDM.

2. Przedmiot zamówienia

1. Przeprowadzenie audytu spełnienia obligatoryjnych kryteriów ankiety weryfikacji dojrzałości w zakresie cyberbezpieczeństwa.
2. Opracowanie raportu zgodności z ankietą, obejmującego każde kryterium obligatoryjne.
3. Opracowanie rekomendacji działań naprawczych dla kryteriów niespełnionych lub spełnionych częściowo.
4. Przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla kadry kierowniczej oraz pracowników Zamawiającego.
5. Przekazanie dokumentacji potwierdzającej realizację szkoleń, w szczególności programu, materiałów, list obecności, certyfikatów lub zaświadczeń oraz raportu ze szkoleń.

3. Cel zamówienia

- weryfikacja spełnienia obligatoryjnych wymagań ankiety dojrzałości cyberbezpieczeństwa,
- identyfikacja braków, ryzyk i niezgodności względem kryteriów obligatoryjnych,
- przygotowanie Zamawiającego do audytu końcowego i odbioru projektu w obszarze cyberbezpieczeństwa,
- podniesienie świadomości cyberzagrożeń wśród pracowników,
- przygotowanie kadry kierowniczej do podejmowania decyzji w przypadku cyberincydentu,
- udokumentowanie spełnienia wymagań dotyczących szkoleń wskazanych w ankiecie.

4. Zakres audytu cyberbezpieczeństwa

4.1. Zasada podstawowa

Audyt cyberbezpieczeństwa obejmuje weryfikację wszystkich kryteriów oznaczonych jako obligatoryjne w kolumnie „Czy obligatoryjne?” ankiety weryfikacji dojrzałości w zakresie

cyberbezpieczeństwa. Kryteria nieobligatoryjne nie stanowią podstawowego zakresu audytu i mogą zostać ujęte wyłącznie informacyjnie, jeżeli Wykonawca uzna to za niezbędne dla przedstawienia kontekstu bezpieczeństwa lub zależności pomiędzy wymaganiami.

Dla każdego kryterium obligatoryjnego Wykonawca dokona oceny na podstawie dokumentacji, konfiguracji, wyników testów, wywiadów, zrzutów ekranowych, raportów systemowych, potwierdzeń szkoleniowych lub innych dowodów przedstawionych przez Zamawiającego.

4.2. Obszary i kryteria obligatoryjne objęte audytem

Lp.	Obszar	Zakres obligatoryjny do weryfikacji
1	System kopii zapasowych	Odmiejscowione kopie zapasowe, aktualne wsparcie producenta, kopie kluczowych systemów, separacja infrastruktury backupu od środowiska produkcyjnego, testy odtworzenia, dokumentacja powdrożeniowa, instruktaż administratorów.
2	Zapory sieciowe	Ochrona przed złośliwym oprogramowaniem dla ruchu z/do Internetu, IPS/IDS, filtrowanie zawartości i kategorii treści, firewall brzegowy oraz podział sieci na podsieci, zmiana haseł domyślnych, wyłączenie nieużywanych portów/usług/kont, ograniczenie dostępu administracyjnego, procedura backupu konfiguracji, kompetencje administratorów.
3	Ochrona poczty e-mail	SPF, DMARC i DKIM, ochrona antyspam i antymalware, testy mechanizmów ochrony poczty, obowiązkowy drugi składnik uwierzytelniający dla poczty dostępnej z sieci publicznej, kompetencje administratorów, regularna kopia bezpieczeństwa poczty.
4	Segmentacja sieci	Segmentacja VLAN zapewniająca separację sieci biurowej, serwerowej, systemu kopii zapasowych, urządzeń medycznych i sieci gościnnej oraz reguły bezpieczeństwa pomiędzy segmentami oparte na zasadzie minimalnego niezbędnego dostępu.
5	Ochrona stacji roboczych oraz serwerów / EDR	Ochrona przed złośliwym oprogramowaniem z aktualnym wsparciem, rozwiązanie klasy EDR dla wspieranych stacji roboczych i serwerów, analiza ryzyka dla zasobów nieobjętych ochroną, kompetencje administratorów systemów ochrony.
6	System zarządzania bezpieczeństwem informacji	Polityki: zarządzania dostępem i uprawnieniami, kryptografii, zarządzania podatnościami, zarządzania ryzykiem w cyberbezpieczeństwie, logowania zdarzeń, kopii bezpieczeństwa, zarządzania incydentami, ciągłości działania, ochrony danych osobowych z uwzględnieniem danych medycznych.
7	Szkolenia z zakresu cyberhigieny	Weryfikacja spełnienia wymogu odbycia szkoleń przez kadrę kierowniczą oraz przez co najmniej 75% pracowników biurowych i medycznych pracujących na systemach informatycznych szpitala, w zakresie określonym w ankiecie.

4.3. Obszary nieobligatoryjne

Obszary, w których ankieta nie wskazuje kryteriów obligatoryjnych, nie są objęte obowiązkową oceną zgodności, chyba że Zamawiający zleci ich weryfikację odrębnie. Dotyczy to w szczególności zarządzania podatnościami jako systemu skanowania podatności, usług zarządzanych bezpieczeństwa oraz wybranych wymagań dotyczących uwierzytelniania i autoryzacji do systemów, o ile w ankiecie oznaczono je jako nieobligatoryjne.

5. Sposób przeprowadzenia audytu

1. spotkanie otwierające i uzgodnienie harmonogramu prac,
2. analiza ankiety oraz dokumentacji przedstawionej przez Zamawiającego,
3. wywiady z osobami odpowiedzialnymi za IT, bezpieczeństwo informacji, administrację systemami i zarządzanie jednostką,

4. weryfikacja konfiguracji i dowodów wdrożenia zabezpieczeń w zakresie niezbędnym do oceny kryteriów obligatoryjnych,
5. weryfikacja wyników testów, raportów systemowych, protokołów odtworzeniowych, dokumentacji powykonawczej i umów utrzymaniowych,
6. opracowanie raportu wstępnego zawierającego braki oraz rekomendacje,
7. omówienie wyników z Zamawiającym,
8. opracowanie raportu końcowego i tabeli zgodności.

6. Produkty audytu

- plan audytu i harmonogram prac,
- lista wymaganych dokumentów i dowodów do przedstawienia przez Zamawiającego,
- raport z audytu cyberbezpieczeństwa,
- tabela zgodności z każdym kryterium obligatoryjnym ankiety,
- lista niezgodności i braków,
- analiza ryzyk wynikających z niespełnienia wymagań,
- rekomendacje działań naprawczych wraz z priorytetami,
- prezentacja lub spotkanie podsumowujące wyniki audytu.

7. Minimalna zawartość raportu zgodności z ankietą

Raport zgodności musi zawierać co najmniej:

- numer i nazwę obszaru z ankiety,
- numer kryterium,
- treść kryterium obligatoryjnego,
- wynik oceny: spełnione / niespełnione / spełnione częściowo / nie dotyczy,
- uzasadnienie oceny,
- wskazanie zweryfikowanych dowodów,
- opis stwierdzonych braków,
- ocenę ryzyka lub wpływu braku na spełnienie wymagań projektu,
- rekomendację działań naprawczych,
- priorytet rekomendacji oraz sugerowany termin realizacji.

8. Wymagania dotyczące szkoleń z zakresu cyberbezpieczeństwa

8.1. Cel szkoleń

Celem szkoleń jest spełnienie wymagań ankiety w zakresie podnoszenia świadomości cyberbezpieczeństwa oraz praktyczne przygotowanie pracowników Zamawiającego do bezpiecznej pracy z systemami informatycznymi, rozpoznawania zagrożeń i reagowania na incydenty.

8.2. Grupy szkoleniowe

Lp.	Grupa	Opis grupy	Minimalny wymóg
1	Kadra kierownicza	Osoby zarządzające jednostką, kierownicy komórek organizacyjnych, osoby odpowiedzialne za decyzje organizacyjne w przypadku incydentu.	Szkolenie musi objąć osoby wskazane przez Zamawiającego jako kadrę kierowniczą.

2	Pracownicy biurowi i medyczni	Pracownicy pracujący na systemach informatycznych szpitala, w tym systemach obsługi pacjenta, dokumentacji medycznej, poczty elektronicznej i systemach administracyjnych.	Szkoleniem należy objąć co najmniej 75% pracowników pracujących na systemach informatycznych szpitala.
3	Personel IT / administratorzy	Osoby administrujące systemami, siecią, pocztą, backupem, zabezpieczeniami stacji i serwerów.	Zakres może zostać przeprowadzony jako osobny moduł techniczny lub jako warsztat uzupełniający.

8.3. Minimalny zakres tematyczny szkoleń

Grupa	Minimalny zakres szkolenia
Kadra kierownicza	Podstawy prawne w obszarze cyberbezpieczeństwa; typy ataków; reagowanie na incydenty; wykonywanie badań bezpieczeństwa; rola kadry zarządzającej w procesach bezpieczeństwa; podejmowanie decyzji w sytuacji cyberincydentu; komunikacja kryzysowa; odpowiedzialność organizacyjna.
Pracownicy biurowi i medyczni	Podstawowe zasady cyberhigieny; typy ataków wraz z przykładami; phishing i socjotechnika; bezpieczna praca z pocztą elektroniczną; bezpieczeństwo haseł i uwierzytelnianie; ransomware; bezpieczna praca z dokumentacją medyczną i danymi osobowymi; zgłaszanie incydentów; zasady korzystania z systemów IT.
Personel IT / administratorzy	Zasady bezpiecznej administracji; kopie zapasowe i testy odtworzeniowe; segmentacja i zapory sieciowe; bezpieczeństwo poczty; EDR i ochrona stacji/serwerów; zarządzanie uprawnieniami; logowanie zdarzeń; reagowanie techniczne na incydenty; dokumentowanie działań i dowodów na potrzeby audytu.

8.4. Forma i organizacja szkoleń

- Szkolenia mogą zostać przeprowadzone stacjonarnie, zdalnie lub hybrydowo, zgodnie z ustaleniami z Zamawiającym.
- Wykonawca zapewni program szkolenia, materiały szkoleniowe oraz osoby prowadzące posiadające wiedzę i doświadczenie w obszarze cyberbezpieczeństwa.
- Szkolenia powinny wykorzystywać przykłady zagrożeń typowych dla sektora ochrony zdrowia, w szczególności phishing, ransomware, wyłudzenia danych, błędne udostępnienie danych medycznych i naruszenia ciągłości działania.
- Dla kadry kierowniczej zaleca się element ćwiczenia decyzyjnego typu tabletop, obejmujący scenariusz cyberincydentu w podmiocie leczniczym.
- Dla pracowników biurowych i medycznych szkolenie powinno mieć charakter praktyczny i zawierać przykłady wiadomości phishingowych, zasady zgłaszania incydentów oraz zasady bezpiecznej pracy z systemami.
- Wykonawca uzgodni z Zamawiającym harmonogram szkoleń tak, aby umożliwić udział wymaganej liczby pracowników bez zakłócenia pracy jednostki.

8.5. Minimalny czas trwania

Grupa	Minimalny czas trwania
Kadra kierownicza	minimum 2 godziny szkoleniowe; rekomendowane 3-4 godziny przy realizacji ćwiczenia tabletop
Pracownicy biurowi i medyczni	minimum 1,5 godziny szkoleniowej na grupę; dopuszczalne są powtarzalne edycje dla różnych grup pracowników
Personel IT / administratorzy	minimum 2 godziny szkoleniowe, o ile Zamawiający zleci odrębny moduł techniczny

8.6. Dokumentowanie realizacji szkoleń

Wykonawca zobowiązany jest przekazać Zamawiającemu komplet dokumentów potwierdzających realizację szkoleń, w tym:

- konspekt lub program szkolenia dla każdej grupy,
- materiały szkoleniowe w formie elektronicznej,
- listy obecności albo raporty obecności z platformy szkoleniowej,
- certyfikaty lub zaświadczenia uczestnictwa, jeżeli Zamawiający ich wymaga,
- raport ze szkoleń zawierający liczbę przeszkolonych osób, grupy szkoleniowe, daty, czas trwania i zakres tematyczny,
- oświadczenie lub dane niezbędne do potwierdzenia objęcia szkoleniami co najmniej 75% pracowników pracujących na systemach informatycznych szpitala,
- rekomendacje dotyczące dalszego podnoszenia świadomości cyberbezpieczeństwa.

8.7. Wymagania jakościowe dla szkoleń

- Treści szkoleniowe muszą być aktualne, praktyczne i dostosowane do specyfiki podmiotu leczniczego.
- Szkolenia nie mogą ograniczać się wyłącznie do prezentacji ogólnych definicji; muszą obejmować przykłady realnych sytuacji oraz wskazanie prawidłowych zachowań pracowników.
- Materiały szkoleniowe powinny być przygotowane w języku polskim.
- Prowadzący szkolenie powinien posiadać doświadczenie w prowadzeniu szkoleń z cyberbezpieczeństwa lub bezpieczeństwa informacji.
- Wykonawca powinien umożliwić zadawanie pytań przez uczestników oraz udzielić odpowiedzi w trakcie szkolenia lub w formie podsumowania po szkoleniu.

10. Wymagania wobec Wykonawcy

10.1. Role

- audytor wiodący
- specjalista ds. cyberbezpieczeństwa lub bezpieczeństwa informacji,
- trener / szkoleniowiec z zakresu cyberbezpieczeństwa.

Audytor lub specjalista powinien posiadać certyfikat CISA lub CISSP, CISM, ISO 27001 Lead Auditor, CEH lub inny równoważny certyfikat potwierdzający kompetencje w zakresie audytu bezpieczeństwa informacji, cyberbezpieczeństwa lub testów bezpieczeństwa.

11. Poufność i ochrona danych

- zachowania poufności wszystkich informacji uzyskanych w toku realizacji zamówienia,
- podpisania umowy o poufności, jeżeli Zamawiający tego wymaga,
- wykorzystywania informacji o systemach Zamawiającego wyłącznie w celu realizacji zamówienia,
- zabezpieczenia materiałów, raportów i dowodów audytowych przed dostępem osób nieupoważnionych,
- usunięcia lub zwrotu danych po zakończeniu realizacji zamówienia, zgodnie z ustaleniami z Zamawiającym,
- przestrzegania przepisów o ochronie danych osobowych.

12. Termin i harmonogram realizacji

1. Termin realizacji zamówienia: maksymalnie do [wpisać termin] od dnia podpisania umowy.

2. W terminie 14 dni od podpisania umowy Wykonawca przedstawi harmonogram prac, ale nie później niż do 31 maja 2026 roku.

3. Audyt powinien zostać wykonany przed zakończeniem projektu lub przed terminem wskazanym przez Zamawiającego.

4. Szkolenia powinny zostać przeprowadzone w terminie umożliwiającym udokumentowanie spełnienia wymagań ankiety.

13. Odbiór prac

Podstawą odbioru prac będzie przekazanie i zaakceptowanie przez Zamawiającego następujących produktów:

- raport z audytu cyberbezpieczeństwa,
- tabela zgodności z obligatoryjnymi kryteriami ankiety,
- lista niezgodności i rekomendacje działań naprawczych,
- materiały szkoleniowe,
- listy obecności lub inne dowody uczestnictwa,
- raport ze szkoleń,
- certyfikaty lub zaświadczenia uczestnictwa, jeżeli wymagane,
- prezentacja lub notatka ze spotkania podsumowującego,
- podpisany protokół odbioru.

Warunkiem odbioru audytu jest objęcie oceną wszystkich kryteriów obligatoryjnych z ankiety oraz wskazanie dowodów, na podstawie których dokonano oceny.

14. Kryteria oceny ofert - propozycja

Zamawiający przyjmuje następujące kryterium oceny ofert:

Cena brutto – 100%

Zastosowanie kryterium ceny jako jedynego kryterium oceny ofert jest uzasadnione tym, że w Opisie Przedmiotu Zamówienia określono wymagania jakościowe odnoszące się do głównych elementów przedmiotu zamówienia, w szczególności do:

1. zakresu audytu obejmującego obligatoryjne kryteria ankiety weryfikacji dojrzałości w zakresie cyberbezpieczeństwa,
2. minimalnego zakresu czynności audytowych,
3. wymaganych produktów audytu, w tym raportu zgodności, analizy ryzyka, rekomendacji oraz raportu końcowego,
4. wymagań dotyczących szkoleń, ich zakresu tematycznego, grup uczestników, materiałów szkoleniowych i potwierdzenia uczestnictwa,
5. wymagań dotyczących doświadczenia i kwalifikacji osób skierowanych do realizacji zamówienia,
6. zasad odbioru prac i wymaganych dokumentów odbiorowych.

W przypadku gdy Zamawiający uzna, że dla zapewnienia porównania poziomu oferowanego wykonania zamówienia zasadne jest zastosowanie kryteriów pozacenowych, może zastosować dodatkowe kryteria jakościowe, pod warunkiem że będą one związane z przedmiotem zamówienia, mierzalne, jednoznacznie opisane oraz możliwe do zweryfikowania na podstawie treści oferty.