UNIWERSYTECKI DZIECIĘCY SZPITAL KLINICZNY
im. L. Zamenhofa w Białymstoku
Dział Informatyki

Białystok, 08.06.2026 r.

INF/08/2026/MD

Zaproszenie do złożenia oferty

Uniwersytecki Dziecięcy Szpital Kliniczny im. L. Zamenhofa w Białymstoku, ul. J. Waszyngtona 17, zwraca się z prośbą o złożenie oferty na **Przygotowanie dokumentacji pod wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w Uniwersyteckim Dziecięcym Szpitalu Klinicznym im. L. Zamenhofa w Białymstoku**

I. Cel zamówienia:

1. Celem zamówienia jest:

1) zapewnienie zgodności z aktualnymi przepisami prawa polskiego i unijnego, w szczególności RODO, Dyrektywą NIS2 oraz ustawą o krajowym systemie cyberbezpieczeństwa (KSC),

2) podniesienie poziomu bezpieczeństwa informacji i danych w Uniwersyteckim Dziecięcym Szpitalu Klinicznym im. L. Zamenhofa w Białymstoku i jednostkach podległych,

3) przygotowanie organizacji do ewentualnej certyfikacji zgodnej z normą ISO/IEC 27001,

4) ujednolicenie zasad ochrony informacji w całej strukturze Szpitala.

2. Zamawiający oczekuje rozwiązań praktycznych, dostosowanych do struktury i procesów Szpitala, możliwych do wdrożenia i stosowania. Niedopuszczalne jest przekazanie Zamawiającemu jedynie ogólnych wzorów, szablonów lub dokumentów wymagających samodzielnego uzupełnienia po odbiorze. Dokumentacja ma wynikać z audytu, uzgodnień z jednostkami organizacyjnymi oraz faktycznych ryzyk i sposobu pracy Szpitala.

II. Przedmiot i zakres zamówienia:

1. Przedmiotem zamówienia jest wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) wraz z audytem stacjonarnym i opracowaniem kompletnej dokumentacji bezpieczeństwa informacji dla Uniwersyteckiego Dziecięcego Szpitala Klinicznego im. L. Zamenhofa w Białymstoku.

2. Przedmiotem zamówienia jest przeprowadzenie audytu diagnostycznego „zerowego" w Uniwersyteckim Dziecięcym Szpitalu Klinicznym im. L. Zamenhofa w Białymstoku oraz opracowanie i przekazanie kompletnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), przygotowanej na podstawie audytu i uzgodnień z jednostkami organizacyjnymi, wraz z pakietem wdrożeniowym oraz opieką pełnomocnika ds. SZBI. Zamówienie ma zapewnić uporządkowanie zasad bezpieczeństwa informacji i cyberbezpieczeństwa Zamawiającego.

3. Usługi realizowane w ramach przedmiotu zamówienia polegać będą w szczególności na realizacji następujących zadań:

1) Zadanie I – przeprowadzenie audytu diagnostycznego „zerowego" (stacjonarnie) we wszystkich jednostkach Uniwersyteckiego Dziecięcego Szpitala Klinicznego im. L. Zamenhofa w Białymstoku jako element rozpoznania spełniania wymagań organizacyjno-procesowych i technicznych w obszarze

bezpieczeństwa informacji i cyberbezpieczeństwa;
2) Zadanie II – opracowanie, uzupełnienie i dostosowanie do Zamawiającego dokumentacji SZBI (w tym dokumentacji ochrony informacji zawierających dane osobowe), wraz z rejestrami, instrukcjami i pakietem wdrożeniowym;
3) Zadanie III - usługa wdrożenia i wsparcia pełnomocnika ds. SZBI przy utrzymaniu tej dokumentacji po jej wdrożeniu oraz wykonywanie przeglądów całego systemu SZBI w organizacji
4. Zamówienie ma dotyczyć całego Szpitala wraz z jego jednostkami organizacyjnymi (oddziały, poradnie, kliniki, pracownie, administracja, IT, archiwum i inne komórki wskazane przez Zamawiającego). Wykonawca jest zobowiązany zaplanować spotkania w sposób odgórny i skoordynowany, tak aby możliwe było przeprowadzenie audytu i uzgodnień w każdej jednostce organizacyjnej.
5. Wynikiem audytu będzie raport zawierający co najmniej: opis stanu obecnego, wykaz niezgodności i słabości, mapę procesów istotnych dla bezpieczeństwa informacji, listę rekomendacji naprawczych i usprawniających oraz wnioski niezbędne do opracowania dokumentacji SZBI.
III. Szczegółowy zakres zadań do realizacji przez Wykonawcę.
Zadanie I – Przeprowadzenie audytu diagnostycznego „zerowego":
1. W ramach Zadania I Wykonawca przeprowadzi audyt „zerowy" (diagnostyczny) stacjonarnie w wszystkich jednostkach organizacyjnych I siedzibach Zamawiającego.
2. Audyt obejmować będzie co najmniej:
1) wywiady z przedstawicielami każdej jednostki organizacyjnej;
2) oględziny jednostek organizacyjnych wraz z obszarami newralgicznymi w tym dotyczącymi bezpieczeństwa fizycznego i środowiskowego (m.in: serwerownia, archiwum, pomieszczenia administracyjne);
3) ocenę zabezpieczeń technicznych, organizacyjnych oraz fizycznych jednostki;
4) przegląd wybranych ustawień i mechanizmów bezpieczeństwa systemów informatycznych;
5) przegląd praktyk w obszarach: kopii zapasowych, zapory sieciowej, segmentacji sieci, ochrony stacji roboczych i serwerów, zarządzanych usług bezpieczeństwa oraz uwierzytelnienia i autoryzacji;
6) analizę istniejącej dokumentacji, rejestrów i procedur (jeżeli występują) oraz weryfikacja ich zgodności z realną praktyką;
7) weryfikację zgodności organizacyjno-proceduralnej z wymaganiami normatywnymi i dobrymi praktykami przyjętymi przez Zamawiającego.
3. Audyt zerowy ma pozostawać w zgodności z przepisami prawa właściwymi dla Zamawiającego, w szczególności:
a) ustawą o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. 2025 poz. 1703),
b) rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (Dz.U. 2024 poz. 773),
c) rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO),
d) ustawą o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2026 poz. 20),
e) a także przepisami właściwymi dla podmiotów leczniczych, w tym w szczególności ustawą o działalności leczniczej (Dz.U. 2026 poz. 156), ustawą o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz.U. 2024 poz. 581) oraz przepisami wykonawczymi dotyczącymi dokumentacji medycznej (t.j. Dz.U. 2024 poz. 798).
4. Jednocześnie audyt i dokumentacja będą prowadzone w oparciu o aktualne wydania norm z zakresu SZBI i ciągłości działania, w szczególności PN-EN ISO/IEC 27001, PN-EN ISO/IEC 27002, PN-EN

ISO/IEC 27005, PN-EN ISO/IEC 27701, PN-EN ISO/IEC 22301 oraz, w zakresie usług chmurowych, PN-EN ISO/IEC 27017 lub norm równoważnych; z uwzględnieniem norm sektorowych adekwatnych do ochrony informacji medycznej (ISO 27799) oraz, w zakresie sieci obejmującej urządzenia/systemy medyczne, IEC 80001-1, w zakresie adekwatnym do stanu faktycznego Zamawiającego.

5. Audyt „zerowy" będzie uwzględniał co najmniej następujące obszary określone w normie PN-EN ISO/IEC 27001:

1) kontekst organizacji,
2) polityki bezpieczeństwa informacji i inne dokumenty dotyczące bezpieczeństwa informacji,
3) organizacja bezpieczeństwa informacji,
4) postepowanie z ryzykiem w bezpieczeństwie informacji,
5) bezpieczeństwo zasobów ludzkich,
6) zarządzanie aktywami,
7) kontrola dostępu oraz upoważnienia do przetwarzania do danych osobowych,
8) kryptografia,
9) bezpieczeństwo fizyczne i środowiskowe,
10) bezpieczna eksploatacja,
11) bezpieczeństwo komunikacji,
12) pozyskiwanie, rozwój i utrzymanie systemów,
13) relacje z dostawcami,
14) zarządzanie incydentami związanymi z bezpieczeństwem informacji,
15) zarządzanie ciągłością działania.

6. Efektem realizacji Zadania I będzie raport z audytu bezpieczeństwa, przekazany Zamawiającemu w postaci elektronicznej w formacie edytowalnym oraz PDF, zawierający co najmniej:

1) opis wykonania planu audytu;
2) opis wykorzystanych standardów;
3) wykaz zidentyfikowanych luk i niezgodności;
4) rekomendacje działań korygujących i doskonalących;
5) oraz założenia do SZBI (mapa obszarów do uporządkowania, priorytety, właściciele, status działań: zrealizowane/częściowo zrealizowane/niezrealizowane).

7. Zamawiający zastrzega sobie prawo do uwag do zawartości raportu z przeprowadzonego audytu w zakresie realizacji Zadania I. Warunkiem odbioru raportu z przeprowadzonego audytu bezpieczeństwa jest jego akceptacja przez Zamawiającego. Potwierdzeniem wykonania raportu będzie, podpisany z wynikiem pozytywnym przez Strony, Protokół odbioru raportu z przeprowadzonego audytu bezpieczeństwa.

8. Prace w zakresie realizacji Zadania I, wykonawca wykona w terminie do 3 tygodni od daty podpisania umowy.

9. Termin realizacji Zadania I zostanie dotrzymany jeżeli w tym terminie podpisany zostanie Protokół Odbioru Zadania I.

Zadanie II – Opracowanie dokumentacji SZBI:

1. W ramach Zadania II Wykonawca opracuje, uzupełni i dostosuje do Zamawiającego kompletną dokumentację SZBI w oparciu o wyniki audytu „zerowego", uzgodnienia z jednostkami organizacyjnymi oraz stan faktyczny procesów i systemów Szpitala. Dokumentacja ma być praktyczna, spójna oraz gotowa do wdrożenia i stosowania operacyjnego.

2. Zamawiający zastrzega zakaz dostarczenia dokumentacji w postaci ogólnych wzorców/szablonów,

w szczególności dokumentów wymagających uzupełnienia przez Zamawiającego po odbiorze. Każdy dokument ma być opracowany i wypełniony pod Zamawiającego na podstawie audytu i uzgodnień z jednostkami.

3. Dokumentacja SZBI musi uwzględniać wymagania wynikające z norm Normy PN-ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-ISO/IEC 27701, PN-ISO/IEC 27017 oraz PN-ISO/IEC 22301, oraz zapewniać spójność z wymaganiami prawa właściwymi dla Zamawiającego, w tym w szczególności z przepisami o ochronie danych osobowych (RODO), rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (Dz.U. 2024 poz. 773), ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2026 poz. 20 z późn. zm.), a także regulacjami wdrażającymi dyrektywę (UE) 2022/2555 (NIS2) w zakresie mającym zastosowanie do Zamawiającego oraz z wymaganiami dotyczącymi bezpieczeństwa informacji i systemów teleinformatycznych:

4. Dokumentacja SZBI musi uwzględniać wymagania wynikające z norm PN-ISO/IEC 27001 i PN-ISO/IEC 27002 oraz powiązanej z nimi PN-ISO/IEC 27017 i obejmować, w szczególności poniższe obszary:

1) polityka bezpieczeństwa informacji:
a) polityki dotyczące bezpieczeństwa informacji I ochrony danych osobowych,
b) instrukcję zarządzania systemem informatycznym,
c) organizacja bezpieczeństwa informacji:
d) role i odpowiedzialność za bezpieczeństwo informacji,
e) rozdzielanie obowiązków,
f) bezpieczeństwo informacji w zarządzaniu projektami,
g) bezpieczeństwo zasobów ludzkich,
h) warunki zatrudnienia,
i) odpowiedzialność kierownicza,
j) uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji,
2) zarządzanie aktywami:
a) inwentaryzacja aktywów,
b) akceptowalne użycie aktywów,
c) zwrot aktywów,
d) klasyfikacja informacji,
e) znakowanie informacji,
f) postępowanie z aktywami,
g) zarządzanie nośnikami wymiennymi,
h) wycofywanie nośników,
3) ochronę danych osobowych w tym:
a) rejestr czynności przetwarzania danych osobowych (RCP),
b) rejestr umów powierzenia przetwarzania danych osobowych oraz wykaz podmiotów przetwarzających,
c) rejestr udostępnień danych osobowych oraz udostępnień dokumentacji medycznej w zakresie wynikającym z procesów Zamawiającego,
d) rejestr naruszeń ochrony danych osobowych,
e) procedurę obsługi naruszeń ochrony danych osobowych,
f) procedurę zarządzania incydentami bezpieczeństwa informacji w zakresie obejmującym zdarzenia dotyczące danych osobowych,
g) procedurę realizacji praw osób, których dane dotyczą,

h) procedurę oceny ryzyka dla ochrony danych osobowych,
i) procedurę oceny skutków dla ochrony danych (DPIA), w zakresie adekwatnym do procesów Zamawiającego,
j) politykę i procedurę nadawania, zmiany i odbierania upoważnień do przetwarzania danych osobowych,
k) indywidualnie nadane poważnienia do przetwarzania danych osobowych dla personelu Zamawiającego oraz rejestr upoważnień,
l) procedurę zarządzania dostępem i uprawnieniami do systemów przetwarzających dane osobowe,
m) politykę retencji danych osobowych oraz procedurę usuwania i niszczenia danych oraz nośników,
n) procedurę weryfikacji, dopuszczania i nadzorowania podmiotów przetwarzających oraz procedurę powierzania przetwarzania danych,
o) procedurę udostępniania danych podmiotom zewnętrznym, w tym organom i instytucjom uprawnionym,
p) procedurę privacy by design i privacy by default w zakresie projektowania i zmian procesów oraz systemów,
q) politykę i procedurę monitoringu wizyjnego,
r) procedurę przechowywania, zabezpieczania i archiwizacji dokumentacji zawierającej dane osobowe, w tym dokumentacji medycznej, w zakresie adekwatnym do procesów Zamawiającego,
4) przekazywanie nośników kontrola dostępu:
a) polityka kontroli dostępu,
b) procedura nadawania i odbierania upoważnień do przetwarzania danych oraz uprawnień w systemach informatycznych,
c) dostęp do sieci i usług sieciowych,
d) rejestrowanie i wyrejestrowywanie użytkowników,
e) przydzielanie dostępu użytkownikom,
f) zarządzanie prawami uprzywilejowanego dostępu,
g) zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników,
h) przegląd praw dostępu użytkowników,
i) odbieranie lub dostosowywanie praw dostępu,
j) stosowanie poufnych informacji uwierzytelniających,
k) ograniczanie dostępu do informacji,
l) procedury bezpieczeństwa logowania,
m) system zarządzania hasłami,
n) użycie uprzywilejowanych programów narzędziowych,
5) kryptografia:
a) polityka stosowania zabezpieczeń kryptograficznych,
b) zarządzanie kluczami, uprawnieniami i dostępem do kluczy,
6) bezpieczeństwo fizyczne i środowiskowe:
a) fizyczna granica obszaru bezpiecznego,
b) ochrona przed zagrożeniami zewnętrznymi i środowiskowymi,
c) praca w obszarach bezpiecznych,
d) dostawy,
e) lokalizacja i ochrona sprzętu,
f) bezpieczeństwo okablowania,
g) konserwacja sprzętu,

h) bezpieczne zbywanie lub przekazywanie do ponownego użycia,
i) polityka czystego biurka i ekranu,
7) bezpieczna eksploatacja:
a) dokumentowanie procedur eksploatacyjnych,
b) zabezpieczenia przed szkodliwym oprogramowaniem,
c) kopie zapasowe,
d) rejestrowanie zdarzeń i incydentów,
e) ochrona informacji w dziennikach zdarzeń,
f) rejestrowanie działań administratorów i operatorów,
g) zarządzanie podatnościami technicznymi,
h) ograniczenia w instalowaniu oprogramowania,
8) bezpieczeństwo komunikacji:
a) zabezpieczenia sieci,
b) polityki i procedury przesyłania informacji,
c) porozumienia dotyczące przesyłania informacji,
d) regulamin pracy zdalnej,
e) umowy o zachowaniu poufności lub nieujawnieniu informacji,
9) pozyskiwanie, rozwój i utrzymanie systemów:
a) analiza i specyfikacja wymagań związanych z bezpieczeństwem informacji,
b) zabezpieczanie usług aplikacyjnych w sieciach publicznych,
c) ochrona transakcji usług aplikacji,
d) polityka bezpieczeństwa prac rozwojowych,
e) ograniczenia dotyczące zmian w pakietach oprogramowania,
f) outsourcing,
g) relacje z dostawcami,
h) bezpieczeństwo informacji w relacji z dostawcami,
10) zarządzanie incydentami związanymi z bezpieczeństwem informacji i ochroną danych osobowych:
a) odpowiedzialność i procedury,
b) zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i ochroną danych osobowych,
c) ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem,
d) reagowanie na incydenty związane z bezpieczeństwem informacji,
e) wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji,
11) bezpieczeństwo informacji w zarządzaniu ciągłością działania:
a) planowanie ciągłości bezpieczeństwa informacji,
b) wdrożenie ciągłości bezpieczeństwa informacji,

5. Dokumentacja musi być kompatybilna z wdrażanymi lub planowanymi rozwiązaniami technicznymi Zamawiającego.

6. Wykonawca w dokumentacji określi minimalne zasady eksploatacji, nadzoru, raportowania, przeglądów i testów związanych z powyższymi obszarami. W szczególności dokumenty takie jak: rejestr czynności przetwarzania (RCP), analiza ryzyka, rejestry operacyjne, procedury incydentów i naruszeń, zasady zarządzania monitoringiem wizyjnym i kluczami, retencji, udostępnień dokumentacji medycznej oraz zasady dostępu do systemów muszą wynikać z realnych procesów Zamawiającego. Dokumenty muszą odzwierciedlać rzeczywisty podział ról, odpowiedzialności, przepływ informacji oraz faktycznie wykorzystywane systemy.

7. Dokumentacja SZBI będzie wykonana w oparciu o aktualne wydania (w tym wdrożenia krajowe

PN/PN-EN) norm z zakresu SZBI, zarządzania ryzykiem oraz ciągłości działania, w szczególności: PN-EN ISO/IEC 27001, PN-EN ISO/IEC 27002, PN-EN ISO/IEC 27005, PN-EN ISO/IEC 27701, PN-EN ISO/IEC 22301, a w zakresie usług chmurowych także PN-EN ISO/IEC 27017, lub norm równoważnych. Dodatkowo, ze względu na specyfikę podmiotu leczniczego, dokumentacja uwzględni wytyczne dla ochrony informacji medycznej wynikające z ISO 27799 oraz, w zakresie infrastruktury sieciowej obejmującej urządzenia/systemy medyczne, wymagania IEC 80001-1, w zakresie adekwatnym do stanu faktycznego Zamawiającego.

8. Zamawiający zastrzega sobie prawo do wniesienia uwag do treści dokumentacji SZBI, zgłaszanych w trakcie procedury odbiorowej.

9. Potwierdzeniem wykonania dokumentacji SZBI będzie podpisany będzie, podpisany z wynikiem pozytywnym przez Strony, protokół odbioru dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji. Zamawiający zastrzega termin realizacji Zadania II maksymalnie do 5 tygodni tygodni od dnia podpisania umowy, jednak nie później niż do dnia 15 lipca 2026 r.

Zadanie III - usługa wdrożenia I wsparcia pełnomocnika ds. SZBI przy utrzymaniu tej dokumentacji po jej wdrożeniu oraz wykonywanie przeglądów całego systemu SZBI w organizacji;

1. Po opracowaniu i odbiorze dokumentacji SZBI Wykonawca zapewni Zamawiającemu usługi wsparcia pełnomocnika ds. SZBI celem dostosowywania przygotowanej dokumentacji oraz jej utrzymania w Szpitalu.

2. Usługi wsparcia świadczone będą w terminie jednego roku od dnia odbioru z wynikiem pozytywnym zaktualizowanej lub opracowanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

3. Usługi, o których mowa w pkt 1, realizowane będą każdorazowo w maksymalnej liczbie godzin 50 roboczogodzin na wniosek Zamawiającego i polegać będą w szczególności na:

1) wdrożeniu, nadzoru i ciągłego doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji oraz zapewnienie zgodności Systemu Zarządzania Bezpieczeństwem Informacji z wymaganiami normy, PN-ISO/IEC 27001:2007, Ustawą o Krajowych Ramach Interoperacyjności, Ustawą o Krajowym Systemie Cyberbezpieczeństwa ,

2) planowaniu i koordynacji prac w zakresie utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji,

3) nadzorowania realizacji działań korygujących i zapobiegawczych wynikających z Zadania I (audytu zerowego),

4) wykonaniu półrocznego i rocznego przeglądu całego systemu SZBI w Szpitalu.

IV. Odbiór przedmiotu zamówienia:

1. W ramach procedury odbioru dokumentacji Zadania I:

1) Wykonawca, przekaże drogą elektroniczną, na adres poczty elektronicznej osoby odpowiedzialnej za realizację Umowy ze strony Zamawiającego przygotowany raport z przeprowadzonego audytu „zerowego", nie później niż 7 dni przed datą zakończenia realizacji Zadania I, celem jego akceptacji,

2) Zamawiający w terminie do 7 dni roboczych od przekazania przez Wykonawcę raportu z przeprowadzonego audytu bezpieczeństwa, powiadomi Wykonawcę, o jego akceptacji lub braku akceptacji i konieczności wprowadzenia zmian;

3) Wykonawca będzie miał prawo, aby ustosunkować się do uwag Zamawiającego w formie pisemnej, przekazując swoje stanowisko na adres poczty elektronicznej osoby odpowiedzialnej za realizację Umowy ze strony Zamawiającego.

4) Zamawiający dopuszcza zorganizowanie spotkań on-line (za pomocą komunikatora internetowego), w celu omówienia koniecznych do wprowadzenia zmian, wskazanych przez

Zamawiającego, z zastrzeżeniem, że spotkanie będzie obligatoryjne, w przypadku jeżeli zażąda tego Zamawiający.

5) Po uzgodnieniu zakresu zmian, Wykonawca wprowadzi je, w terminie do 5 dni roboczych od daty ich uzgodnienia i ponownie przedstawi Zamawiającemu raport z przeprowadzonego audytu bezpieczeństwa, w celu jego akceptacji.

6) Zamawiający zastrzega sobie prawo do dwukrotnego zgłoszenia zmian w przekazanym raporcie z przeprowadzonego audytu bezpieczeństwa.

7) Komunikacja pomiędzy Zamawiającym a Wykonawcą w zakresie akceptacji raportu z przeprowadzonego audytu bezpieczeństwa odbywać się będzie drogą elektroniczną na adresy poczty elektronicznej Wykonawcy i Zamawiającego, wskazane w umowie.

8) W przypadku, gdy przekazany Zamawiającemu powtórnie poprawiony raport z przeprowadzonego audytu bezpieczeństwa nadal nie będzie uwzględniać wyników uzgodnień i uwag Zamawiającego, Zamawiający zastrzega sobie prawo do odmowy odbioru raportu z przeprowadzonego audytu bezpieczeństwa i odstąpienia od Umowy z winy Wykonawcy.

9) W przypadku, o którym mowa w ppkt 8), Zamawiający może zlecić wykonanie raportu z przeprowadzonego audytu bezpieczeństwa podmiotowi trzeciemu, a kosztami obciążyć Wykonawcę.

10) Potwierdzeniem wykonania raportu z przeprowadzonego audytu bezpieczeństwa, będzie podpisany z wynikiem pozytywnym przez osoby odpowiedzialne za realizację Umowy ze strony Wykonawcy i Zamawiającego, wskazane w umowie, Protokół odbioru raportu z przeprowadzonego audytu bezpieczeństwa.

11) Zaakceptowana dokumentacja wytworzona w ramach Zadania I zostanie przygotowana w języku polskim i przekazana Zamawiającemu najpóźniej w dniu odbioru Zadania I, w formie:

 papierowej, w 1 egzemplarzu oraz formie elektronicznej na adres poczty elektronicznej Zamawiającego wskazany w umowie, w formacie plików do edycji i PDF.

2. W ramach procedury odbioru dokumentacji Zadania II:

1) Wykonawca, przekaże drogą elektroniczną, na adres poczty elektronicznej osoby odpowiedzialnej za realizację Umowy ze strony Zamawiającego, wskazany w umowie, przygotowaną zaktualizowaną lub opracowaną dokumentację Systemu Zarządzania Bezpieczeństwem Informacji, nie później niż 15 dni roboczych przed terminem opracowania dokumentacji SZBI, o którym mowa w pkt. II ust. 9, celem jej akceptacji.

2) Zamawiający w terminie do 7 dni roboczych od przekazania przez Wykonawcę zaktualizowanej lub opracowanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, powiadomi Wykonawcę, o jego akceptacji lub braku akceptacji i konieczności wprowadzenia zmian.

3) Wykonawca w terminie 5 dni roboczych będzie miał prawo, aby ustosunkować się do uwag Zamawiającego w formie pisemnej, przekazując swoje stanowisko na adres poczty elektronicznej osoby odpowiedzialnej za realizację Umowy ze strony Zamawiającego, wskazany w umowie.

4) Zamawiający dopuszcza zorganizowanie spotkań on-line (za pomocą komunikatora internetowego), w celu omówienia koniecznych do wprowadzenia zmian, wskazanych przez Zamawiającego, z zastrzeżeniem, że spotkanie będzie obligatoryjne, w przypadku jeżeli zażąda tego Zamawiający.

5) Po uzgodnieniu zakresu zmian, Wykonawca wprowadzi je, w terminie do 3 dni roboczych od daty ich uzgodnienia i ponownie przedstawi Zamawiającemu zaktualizowaną lub opracowaną dokumentację Systemu Zarządzania Bezpieczeństwem Informacji, w celu jej akceptacji.

6) Zamawiający zastrzega sobie prawo do dwukrotnego zgłoszenia zmian w przekazanej zaktualizowanej lub opracowanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

7) Komunikacja pomiędzy Zamawiającym a Wykonawcą w zakresie akceptacji zaktualizowanej lub opracowanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji odbywać się będzie drogą elektroniczną na adresy poczty elektronicznej Wykonawcy i Zamawiającego, wskazane w umowie.
8) W przypadku, gdy przekazana Zamawiającemu powtórnie poprawiona zaktualizowana lub opracowana dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji nadal nie będzie uwzględniać wyników uzgodnień i uwag Zamawiającego, Zamawiający zastrzega sobie prawo do odmowy jej odbioru i odstąpienia od Umowy z winy Wykonawcy;
9) W przypadku, o którym mowa w ppkt. 8) Zamawiający może zlecić wykonanie zaktualizowanej lub opracowanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, a kosztami obciążyć Wykonawcę.
10) Potwierdzeniem wykonania zaktualizowanej lub opracowanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, będzie podpisany z wynikiem pozytywnym przez osoby odpowiedzialne za realizację umowy ze strony Wykonawcy i Zamawiającego, wskazane w umowie, Protokołu odbioru zaktualizowanej lub opracowanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.
11) Zamawiający dokona odbioru ww. dokumentacji jeśli Wykonawca wykonał ją w całości,
a Zamawiający nie będzie wnosił do niej uwag.
12) Zaakceptowana dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji zostanie przygotowana w języku polskim i przekazana Zamawiającemu najpóźniej w dniu jej odbioru w formie: papierowej, w 1 egzemplarzu oraz formie elektronicznej na adres poczty elektronicznej Zamawiającego wskazany w umowie, w formacie plików do edycji i PDF.
3. Zadania I i zadania II mają zostać wykonane najpóźniej do dnia 15 lipca 2026 r.
4. Potwierdzeniem zrealizowania Zadania I i II będzie podpisany z wynikiem pozytywnym przez Strony Końcowy protokół odbioru w terminie do dnia 15 lipca 2026 r.
5. Zadanie III wykonywane będzie w terminie 365 dni od daty odbioru dokumentacji SZBI. Odbiór Zadania III nastąpi po wykonaniu przeglądu rocznego SZBI. Potwierdzeniem odbioru jest Protokół Odbioru Zadania III.
V. Prawa autorskie:
1. Wykonawca przenosi na Zamawiającego, w ramach wynagrodzenia umownego i z chwilą podpisania protokołu odbioru (częściowego lub końcowego) z wynikiem pozytywnym, autorskie prawa majątkowe do wszystkich utworów powstałych w związku z realizacją zamówienia, w szczególności do raportów, polityk, procedur, instrukcji, rejestrów, analiz, materiałów szkoleniowych oraz ich wersji roboczych, a także do plików źródłowych w formatach edytowalnych.
2. Przeniesienie praw następuje na następujących polach eksploatacji: utrwalanie i zwielokrotnianie dowolną techniką (w tym cyfrową); wprowadzanie do pamięci urządzeń i systemów informatycznych Zamawiającego oraz do jego baz danych; rozpowszechnianie, udostępnianie i przekazywanie, w tym w sieci wewnętrznej Zamawiającego oraz podmiotom uprawnionym (np. audytorom, jednostkom certyfikującym, organom publicznym, podmiotom świadczącym usługi na rzecz Zamawiającego) w zakresie niezbędnym do realizacji zadań Zamawiającego; publiczne wyświetlanie i prezentacja; a także tworzenie opracowań, modyfikacji, aktualizacji, adaptacji oraz łączenie z innymi utworami i korzystanie z nich.
3. Zamawiający jest uprawniony do wykonywania autorskich praw zależnych do utworów, o których mowa powyżej, bez prawa Wykonawcy do dodatkowego wynagrodzenia. Przeniesienie praw następuje bez ograniczeń czasowych i terytorialnych.

I. Oferta ma zawierać:

1. Nazwę oraz adres kontaktowy
2. Informację, czego dotyczy
3. Kwotę netto PLN, kwotę brutto PLN oraz stawkę podatku VAT w %
4. Kwota podana w ofercie powinna zawierać wszystkie koszty Wykonawcy związane z realizacją przedmiotu zamówienia, niezbędne dla prawidłowego i pełnego jego wykonania oraz uwzględniać wszelkie opłaty, a także podatki wynikające z realizacji zamówienia, jak również ewentualne upusty i rabaty skalkulowane przez Wykonawcę.

II. Termin złożenia oferty:

Ofertę należy złożyć do 12.06.2026 r. do godz. 15:00 drogą mailową na adres md@udsk.pl

1. Kryterium oceny oferty: 100% cena
2. Osoba kontaktowa: Michał Dojlido tel. 501515712 md@udsk.pl
3. Termin związania ofertą wynosi 7 dni od upływu terminu składania ofert.