Bydgoszcz, 02.06.2026 r.

Nazwa oraz adres Zamawiającego:
Szpital Kliniczny im. dr. Emila Warmińskiego
Politechniki Bydgoskiej - SPZOZ w Bydgoszczy
ul. Szpitalna 19
85-826 Bydgoszcz
telefon: 52 370 91 24
adres poczty elektronicznej: zp2@szpital.pbs.edu.pl
KRS 0000057250; NIP 953-22-93-970, REGON 092354746

znak sprawy: PK-VI-1-2026

Zaproszenie do składania ofert

1. Szpital Kliniczny im. dr. Emila Warmińskiego Politechniki Bydgoskiej - SPZOZ w Bydgoszczy zaprasza Państwa do składania ofert w postępowaniu o wartości netto nieprzekraczającej równowartości 170.000,00 zł którego przedmiotem jest ***„Aktualizacja polityk bezpieczeństwa wraz z audytem końcowym”.***
2. Przedmiotowe postępowanie współfinansowane jest w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (KPO), Komponent D „Efektywność, dostępność i jakość systemu ochrony zdrowia", Inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia", Tytuł Przedsięwzięcia: Transformacja cyfrowa Szpitala Klinicznego im. dr. Emila Warmińskiego Politechniki Bydgoskiej - SPZOZ w Bydgoszczy.
3. Warunki realizacji zamówienia

1	Nazwa przedmiotu zamówienia / parametry lub funkcje przedmiotu umowy	1. Przedmiot zamówienia i podstawa prawna Przedmiotem zamówienia jest usługa polegająca na aktualizacji i dostosowaniu wewnętrznych polityk oraz procedur bezpieczeństwa oraz przeprowadzeniu pełnego audytu bezpieczeństwa informacji i systemów teleinformatycznych, zgodnie z opisanym poniżej zakresem: Audyt końcowy projektu KPO: Weryfikacja realizacji przedsięwzięcia finansowanego z Krajowego Planu Odbudowy. Audyt zgodności z wymaganiami ustawowymi: Weryfikacja wypełniania obowiązków wynikających z Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r., ze szczególnym uwzględnieniem nowelizacji z dnia 23 stycznia 2026 r. oraz właściwych aktów wykonawczych. 2. Cele realizacji audytu Głównym celem usługi jest dostarczenie obiektywnego zapewnienia o poziomie bezpieczeństwa cyfrowego placówki poprzez: 2.1. Ocenę zgodności organizacji z aktualnym stanem prawnym i regulacyjnym.

		2.2. Identyfikację luk w Systemie Zarządzania Bezpieczeństwem Informacji (SZBI) oraz ocenę skuteczności zabezpieczeń technicznych i organizacyjnych. 2.3. Potwierdzenie prawidłowości wydatkowania środków w ramach projektu KPO oraz osiągnięcia założonych wskaźników. 2.4. Opracowanie planu działań naprawczych i rekomendacji optymalizacyjnych. UWAGA: Przed przystąpieniem do realizacji audytu, Wykonawca oraz audytorzy zobowiązani są do podpisania umowy/oświadczenia o zachowaniu poufności (NDA). 3. Szczegółowy zakres audytu KSC Audytorzy zobowiązani są do oceny faktycznego funkcjonowania zabezpieczeń (nie tylko analizy dokumentacji) w następujących domenach: 3.1. Ład organizacyjny i zarządzanie a) Weryfikacja ról i odpowiedzialności kadry zarządzającej, działu IT, Inspektora Ochrony Danych (IOD) oraz podmiotów zewnętrznych. b) Ocena zaangażowania kierownictwa w proces zarządzania ryzykiem oraz procesy decyzyjne. c) Funkcjonowanie Komitetu Bezpieczeństwa oraz polityka zarządzania zasobami ludzkimi. 3.2. SZBI i dokumentacja a) Przegląd kompletności i adekwatności procedur: nadawania uprawnień, polityk haseł/MFA, kopii zapasowych oraz planów ciągłości działania (BCP / Planu Odzyskiwania po Awarii (DRP)). b) Ocena zasad współpracy z dostawcami oraz procedur klasyfikacji zasobów i danych. 3.3. Zarządzanie ryzykiem i środki techniczne a) Ocena metodyki identyfikacji aktywów krytycznych i analizy ryzyka. b) Weryfikacja realnych zabezpieczeń IT: segmentacja sieci, bezpieczeństwo urządzeń końcowych i medycznych, ochrona poczty elektronicznej oraz systemów backupu (w tym kopie immutable/offline). c) Ochrona przed ransomware, zarządzanie podatnościami oraz kontrola dostępu uprzywilejowanego. 3.4. Incydenty i ciągłość działania a) Weryfikacja gotowości do wykrywania incydentów, ścieżek eskalacji oraz współpracy z właściwym CSIRT. b) Ocena zdolności do pracy w trybie degradacji oraz analiza wpływu

		niedostępności systemów na procesy medyczne. 4. Szczegółowy zakres audytu końcowego projektu KPO UWAGA: W przypadku, gdy audytorzy będą mieli dostęp do danych osobowych, konieczne będzie zawarcie umowy powierzenia przetwarzania danych osobowych z administratorem danych. 4.1. Audyt powinien obejmować przynajmniej obszary, w których przetwarzane są dane osobowe wrażliwe, w tym kluczowe systemy informacji medycznej oraz infrastrukturę urządzeń medycznych (aparatura medyczna wraz z systemami je obsługującymi). Audyt powinien obejmować niezbędną infrastrukturę teleinformatyczną podmiotu, w tym przynajmniej bezpieczeństwo takich elementów jak: a) Kanały komunikacji jak np. poczta b) Sieciowe urządzenia brzegowe wraz z zasadami segmentacji oraz przepływów c) Kontrolery domeny d) Platforma wirtualizacyjna e) System zarządzania kopiami zapasowymi f) Poprawność konfiguracji stacji roboczych oraz serwerów g) Sposoby uwierzytelniania się użytkowników 4.2. Audyt musi potwierdzić, że wdrożone rozwiązania funkcjonują w środowisku produkcyjnym i zabezpieczają kluczowe obszary przetwarzania danych medycznych. Zakres obejmuje infrastrukturę teleinformatyczną, w tym: a) Prawidłowość konfiguracji sieciowych urządzeń brzegowych, kontrolerów domeny i platform wirtualizacyjnych. b) Weryfikację systemów zarządzania kopiami zapasowymi oraz metod uwierzytelniania użytkowników. c) Ocenę trwałości rezultatów projektu oraz zgodności z dokumentacją konkursową i umową o dofinansowanie. 5. Wymagania wobec Wykonawcy Wykonawca musi wykazać się potencjałem kadrowym i doświadczeniem umożliwiającym rzetelną realizację zamówienia: Certyfikacja personelu: W skład zespołu audytowego muszą wchodzić osoby posiadające certyfikaty z zakresu norm: ISO 27001 (System Zarządzania Bezpieczeństwem Informacji). ISO 22301 (Zarządzanie Ciągłością Działania). ISO 42001 (System Zarządzania Sztuczną Inteligencją – kluczowy aspekt w

		audytach realizowanych w 2026 r.). Zespół audytujący: co najmniej dwóch audytorów posiadających certyfikaty określone w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 r, poz. 1999) lub co najmniej dwóch audytorów posiadających co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych lub jednostka oceniająca zgodność, akredytowana zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2025 r. poz. 568 z późn.zm.), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych. Audytor wskazany do zadania związanego z aktualizacją i dostosowaniem wewnętrznych polityk oraz procedur musi posiadać certyfikat ISO/IEC 27001, jednocześnie osoba ta nie może zostać wskazana do realizacji audytu. 6. Produkty końcowe Wykonawca dostarczy Raport z Audytu, który musi zawierać: a) Szczegółowy opis stanu faktycznego wraz z identyfikacją podatności. b) Analizę ryzyka dla stwierdzonych niezgodności. c) Rekomendacje naprawcze uszeregowane według priorytetów wdrożenia. d) Wypełnioną ankietę dojrzałości cyberbezpieczeństwa, zgodną ze wzorem stanowiącym załącznik nr 3 do niniejszego zaproszenia, zawierającą kryteria akceptacji stosowane przy ocenie w ramach audytu końcowego w obszarze cyberbezpieczeństwa. 7. W ramach wynagrodzenia ryczałtowego Wykonawca zobowiązany będzie w terminie do 2 miesięcy od dnia zakończenia Audytu do jednorazowej aktualizacji wewnętrznych polityk oraz procedur bezpieczeństwa z uwzględnieniem potrzeb i uwag Zamawiającego.
2	Termin realizacji zamówienia	Przedmiot zamówienia musi zostać zrealizowany w terminie do 10.07.2026 r., w pierwszej kolejności należy opracować dokumentację, a następnie przeprowadzić audyt.
3	Warunki gwarancyjne i serwisowe	Nie dotyczy.
4	Inne warunki ustalone przez zamawiającego	1. Wykonawca zawrze umowę z Zamawiającym, której wzór stanowi załącznik nr 4 do niniejszego zaproszenia. 2. Podstawy wykluczenia. Zamówienie nie może być udzielone: 1) osobom zatrudnionym jednocześnie w instytucji uczestniczącej w realizacji Programu (którego dotyczy ww. Przedsięwzięcie) na podstawie stosunku pracy, chyba że nie zachodzi konflikt interesów lub podwójne finansowanie; 2) osobom/podmiotom powiązanym z Zamawiającym osobowo. Przez powiązania osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przygotowaniem

		i przeprowadzeniem procedury wyboru wykonawcy a wykonawcą, polegające w szczególności na pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli; 3) osobom/podmiotom podlegającym wykluczeniu z postępowania o udzielenie zamówienia na podstawie art. 7 ust. 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego z dnia 13.04.2022 r. 4) Wykonawca wraz z ofertą złoży oświadczenie o braku podstaw do wykluczenia – załącznik nr 2 do zaproszenia. 3. Podstawy odrzucenia ofert. Zamawiający odrzuci ofertę, jeżeli: 1) jest nieważna na podstawie odrębnych przepisów; 2) została złożona po terminie składania ofert; 3) jej treść nie odpowiada treści zaproszenia do składania ofert. 4. Wykonawca zobowiązany jest do realizacji przedmiotu zamówienia w sposób zgodny z zasadą „nie czyń poważnych szkód" (DNSH), o której mowa w przepisach dotyczących zrównoważonego rozwoju oraz taksonomii UE. W szczególności Wykonawca zapewni, że świadczona Usługa lub konieczność wdrożenia zaleceń wynikających z audytu nie będą powodowały znaczącego negatywnego wpływu na środowisko naturalne. W ramach realizacji zamówienia Wykonawca zobowiązany jest w szczególności do: 1) stosowania rozwiązań informatycznych sprzyjających efektywności energetycznej, w tym korzystania z infrastruktury IT o obniżonym zużyciu energii (np. energooszczędne centra danych), 2) optymalizacji działania platformy pod kątem minimalizacji zużycia zasobów (transfer danych, moc obliczeniowa), 3) zapewnienia, że wykorzystywana infrastruktura hostingowa spełnia standardy środowiskowe lub posiada stosowne certyfikaty (np. dotyczące efektywności energetycznej), 4) ograniczania negatywnego wpływu cyklu życia usług cyfrowych poprzez stosowanie dobrych praktyk w zakresie projektowania i utrzymania oprogramowania, 5) niewprowadzania rozwiązań, które mogłyby prowadzić do nadmiernego zużycia energii, generowania zbędnych danych lub innych negatywnych oddziaływań środowiskowych. 5. Wykonawca zobowiązany jest do realizacji przedmiotu zamówienia z zachowaniem zgodności z zasadą równości szans i niedyskryminacji oraz zasadą równości szans kobiet i mężczyzn.

4. Oferty należy przesłać na adres e-mail: **zp2@szpital.pbs.edu.pl** w terminie do dnia: **09.06.2026 r., do godziny: 11:00.** Wzór formularza oferty stanowi załącznik nr 1 do niniejszego zaproszenia. Zamawiający dopuszcza złożenie oferty na formularzu o odmiennej treści niż wskazany wzór, pod warunkiem że dokument ten będzie zawierał co najmniej: oznaczenie (identyfikację) wykonawcy składającego ofertę, dane umożliwiające jego jednoznaczne ustalenie, a także wszystkie elementy niezbędne do dokonania oceny oferty zgodnie z przyjętymi kryteriami oceny ofert.

5. Cena łączna jest całkowitym wynagrodzeniem za zrealizowanie całości zamówienia objętego niniejszym postępowaniem. W cenie uwzględnia się podatek od towarów i usług oraz ewentualnie inne podatki, jeżeli odpowiednie przepisy tego wymagają. W cenie należy uwzględnić wszystkie wymagania określone w niniejszej zaproszeniu oraz wszelkie koszty, jakie poniesie Wykonawca z tytułu należytej oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia, a także wszystkie potencjalne ryzyka ekonomiczne, jakie mogą wystąpić przy realizacji przedmiotu zamówienia.
6. Informacje o środkach komunikacji i sposobie porozumiewania się Zamawiającego z Wykonawcami
   1) Postępowanie prowadzone jest w języku **polskim** przy użyciu środków komunikacji elektronicznej wyłącznie za pośrednictwem poczty e-mail Zamawiającego.
   2) Ofertę oraz inne dokumenty składane wraz z ofertą składa się, pod rygorem nieważności w formie elektronicznej (tj. przy użyciu kwalifikowanego podpisu elektronicznego) lub w postaci elektronicznej, opatrzonej podpisem zaufanym lub podpisem osobistym.
   3) Podpisy kwalifikowane wykorzystywane przez wykonawców do podpisywania wszelkich plików muszą spełniać "Rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku".
   4) W przypadku wykorzystania formatu podpisu XAdES zewnętrzny. Zamawiający wymaga dołączenia odpowiedniej ilości plików tj. podpisywanych plików z danymi oraz plików podpisu w formacie XAdES.
   5) Zgodnie z definicją dokumentu elektronicznego z art. 3 ust. 2 Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, opatrzenie pliku zawierającego skompresowane dane kwalifikowanym podpisem elektronicznym jest jednoznaczne z podpisaniem oryginału dokumentu, z wyjątkiem kopii poświadczonych odpowiednio przez innego wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia, przez podmiot, na którego zdolnościach lub sytuacji polega wykonawca, albo przez podwykonawcę.
   6) Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi max 10MB, oraz na ograniczenie wielkości plików podpisywanych w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi max 5MB.
   7) Składając ofertę zaleca się zaplanowanie złożenia jej z wyprzedzeniem, aby zdążyć w terminie przewidzianym na jej złożenie w przypadku siły wyższej, jak np. awaria Internetu, problemy techniczne, związane z brakiem np. aktualnej przeglądarki, itp.
7. **Kryterium oceny ofert** jest cena łączna za wszystkie Usługi stanowiące przedmiot zamówieinia (100%). Liczba punktów w kryterium cena oferty zostanie wyliczona za pomocą następującego wzoru:

$$Pc = \frac{\text{najniższa zaoferowana cena}}{\text{cena badanej oferty}} \times 100$$

Ofertą najkorzystniejszą będzie oferta z najniższą ceną łączną, spełniająca wymagania

Zamawiającego. Jeżeli nie można dokonać wyboru oferty z uwagi na taką samą ocenę w ww. kryterium, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych zawierających nową cenę.

8. Zamawiający zastrzega sobie prawo do unieważnienia postępowania, na każdym etapie do czasu zawarcia umowy, bez podania przyczyny.

Załączniki:

1. Formularz oferty – zał. nr 1;
2. Wzór oświadczenia dotyczącego braku podstaw wykluczenia z postępowania – zał. nr 2;
3. Ankieta dojrzałości cyberbezpieczeństwa – zał. nr 3;
4. Wzór umowy – zał. nr 4.

Zatwierdzono w dniu:
02-06-2026 r.
Monika Kasprzyk
Dyrektor Naczelna

Signed by / Podpisano przez:
Monika Marta Kasprzyk
Date / Data: 2026-06-02 10:19

Klauzula informacyjna w sprawie ochrony danych osobowych

Zamawiający oświadcza, że spełnia wymogi określone w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) (Dz. Urz. UE L 119 z 4 maja 2016 r.), dalej: RODO, tym samym dane osobowe podane przez Wykonawcę będą przetwarzane zgodnie z RODO oraz zgodnie z przepisami krajowymi.

Zamawiający informuje, że:

1) administratorem danych osobowych Wykonawcy jest Szpital Kliniczny im. dr. Emila Warmińskiego Politechniki Bydgoskiej - SPZOZ w Bydgoszczy, ul. Szpitalna 19, 85-826 Bydgoszcz, tel. (52) 37 09 102, e-mail: sekretariat@szpital.pbs.edu.pl;
2) w sprawach związanych z przetwarzaniem danych osobowych, można kontaktować się z Inspektorem Ochrony Danych, którym jest Pan Jarosław Kwiatkowski, za pośrednictwem telefonu (52) 37 09 133 lub adresu e-mail: iod@szpital.bydgoszcz.pl;
3) dane osobowe Wykonawcy będą przetwarzane w celu przeprowadzenia postępowania o udzielenie zamówienia publicznego pn. „Dostawa i wdrożenie oprogramowania - cyberbezpieczeństwo” – znak sprawy: PK-VI-1-2026 oraz w celu archiwizacji dokumentacji dotyczącej tego postępowania;
4) odbiorcami przekazanych przez Wykonawcę danych osobowych będą osoby lub podmioty, którym zostanie udostępniona dokumentacja postępowania;
5) dane osobowe Wykonawcy będą przechowywane, przez okres 5 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli okres obowiązywania umowy w sprawie zamówienia publicznego przekracza 5 lata, okres przechowywania obejmuje cały okres obowiązywania umowy.

Wykonawca jest zobowiązany, w związku z udziałem w przedmiotowym postępowaniu, do wypełnienia wszystkich obowiązków formalno-prawnych wymaganych przez RODO i związanych z udziałem w przedmiotowym postępowaniu o udzielenie zamówienia. Do obowiązków tych należą:

1) obowiązek informacyjny przewidziany w art. 13 RODO względem osób fizycznych, których dane osobowe dotyczą i od których dane te Wykonawca bezpośrednio pozyskał i przekazał Zamawiającemu w treści oferty lub dokumentów składanych na żądanie Zamawiającego;
2) obowiązek informacyjny wynikający z art. 14 RODO względem osób fizycznych, których dane Wykonawca pozyskał w sposób pośredni, a które to dane Wykonawca przekazuje Zamawiającemu w treści oferty lub dokumentów składanych na żądanie Zamawiającego.

Zamawiający informuje, że:

1) udostępnia dane osobowe, o których mowa w art. 10 RODO (dane osobowe dotyczące wyroków skazujących i czynów zabronionych) w celu umożliwienia korzystania ze środków ochrony prawnej;
2) udostępnianie protokołu i załączników do protokołu ma zastosowanie do wszystkich danych osobowych, z wyjątkiem tych, o których mowa w art. 9 ust. 1 RODO (tj. danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych

genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby), zebranych w toku postępowania o udzielenie zamówienia;

3) w przypadku korzystania przez osobę, której dane osobowe są przetwarzane przez Zamawiającego, z uprawnienia, o którym mowa w art. 15 ust. 1–3 RODO (związanych z prawem Wykonawcy do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jego dotyczące, prawem Wykonawcy do bycia poinformowanym o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem jego danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz prawem otrzymania przez Wykonawcę od administratora kopii danych osobowych podlegających przetwarzaniu), Zamawiający może żądać od osoby występującej z żądaniem wskazania dodatkowych informacji, mających na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia;
4) skorzystanie przez osobę, której dane osobowe są przetwarzane, z uprawnienia, o którym mowa w art. 16 RODO (uprawnienie do sprostowania lub uzupełnienia danych osobowych), nie może naruszać integralności protokołu postępowania oraz jego załączników;
5) w postępowaniu o udzielenie zamówienia zgłoszenie żądania ograniczenia przetwarzania, o którym mowa w art. 18 ust. 1 RODO, nie ogranicza przetwarzania danych osobowych do czasu zakończenia tego postępowania;
6) w przypadku, gdy wniesienie żądania dotyczącego prawa, o którym mowa w art. 18 ust. 1 RODO spowoduje ograniczenie przetwarzania danych osobowych zawartych w protokole postępowania lub załącznikach do tego protokołu, od dnia zakończenia postępowania o udzielenie zamówienia Zamawiający nie udostępnia tych danych, chyba że zachodzą przesłanki, o których mowa w art. 18 ust. 2 rozporządzenia 2016/679.

Załącznik nr 1
wzór

FORMULARZ OFERTY

Zamawiający:
Szpital Kliniczny im. dr. Emila Warmińskiego
Politechniki Bydgoskiej - SPZOZ w Bydgoszczy
ul. Szpitalna 19
85-826 Bydgoszcz

Nazwa Wykonawcy (lub Wykonawców wspólnie ubiegających się o udzielenie zamówienia): ……
……
Adres ……
Nr KRS (jeżeli dotyczy) ……
NIP ……
Wykonawca ☐ JEST ☐ NIE JEST *(zaznaczyć właściwe)* **dużym przedsiębiorcą** w rozumieniu art. 4 pkt 6 ustawy o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych**.**
Osoba do kontaktu ……
Nr telefonu ……
Adres poczty elektronicznej ……

W odpowiedzi zaproszenie do złożenia oferty w postępowaniu pn. **„Aktualizacja polityk bezpieczeństwa wraz z audytem końcowym"** składamy ofertę na wykonanie przedmiotu zamówienia na następujących warunkach:
Cena łączna netto: …… zł

Cena łączna brutto: …… zł

(z dokładnością do dwóch miejsc po przecinku)

Oświadczamy, że:

1) zapoznaliśmy się z warunkami zaproszenia do składania ofert i nie wnosimy do niej żadnych zastrzeżeń;
2) posiadamy wszystkie informacje niezbędne do prawidłowego przygotowania i złożenia niniejszej oferty;
3) zapoznaliśmy się z postanowieniami wzoru umowy, opisem przedmiotu zamówienia i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy zgodnej z niniejszą ofertą, na warunkach określonych w zaproszeniu do składania ofert, w miejscu i terminie wyznaczonym przez Zamawiającego;
4) zapewniamy wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych osobowych spełniało wymogi wynikające z obowiązujących przepisów o ochronie danych osobowych oraz przepisów 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) – dalej „RODO", mających zastosowanie i chroniło prawa osób, których dane dotyczą;

5) znane nam są obowiązki wynikające z obowiązujących przepisów o ochronie danych osobowych i przepisów RODO mających zastosowanie, które zobowiązany jest wykonywać podmiot przetwarzający dane osobowe na zlecenie administratora danych;
6) dopełniliśmy wszelkich obowiązków w stosunku do osób, których dane przekazujemy oraz w stosunku do Zamawiającego wynikających z przepisów o ochronie danych osobowych i przepisów RODO;
7) przekazywane przez nas dane osobowe mogą być wykorzystane wyłącznie w celach związanych z prowadzonym postępowaniem;
8) oświadczamy, że przedmiot zamówienia zamierzamy zrealizować SIŁAMI WŁASNYMI / PRZY UDZIALE PODWYKONAWCÓW *(niepotrzebne skreślić). Jeżeli Wykonawca zamierza zrealizować przedmiot zamówienia przy udziale podwykonawców proszę wypełnić tabelę poniżej:*

Nazwa i adres podwykonawcy *(o ile jest znane Wykonawcy)*	
Zakres zamówienia jaki zostanie powierzony podwykonawcy	
Wartość lub procentowa część zamówienia jaka zostanie powierzona podwykonawcy	

Pozostały zakres zamówienia wykonamy osobiście

Wraz z ofertą składamy:

1. oświadczenie dotyczące braku podstaw wykluczenia z postępowania – załącznik nr 2;
2. ……..

……
podpis osoby reprezentującej Wykonawcę

Załącznik nr 2
wzór

Nazwa Wykonawcy ……
Adres ……

OŚWIADCZENIE WYKONAWCY
dotyczące przesłanek wykluczenia z postępowania

W odpowiedzi na zaproszenie do złożenia oferty w postępowaniu pn. **„Aktualizacja i dostosowanie wewnętrznych polityk oraz procedur bezpieczeństwa oraz przeprowadzenie kompleksowego audytu zgodności z ustawą z dnia 5 lipca 2018 r. o Krajowym systemie cyberbezpieczeństwa (KSC) oraz audytu końcowego projektu Krajowego Programu Odbudowy (KPO)"** oświadczam, że nie podlegam wykluczeniu z uwagi na:

1. Nie jestem zatrudniony jednocześnie w instytucji uczestniczącej w realizacji Przedsięwzięcia pn. „Transformacja cyfrowa Szpitala Klinicznego im. dr. Emila Warmińskiego Politechniki Bydgoskiej – SPZOZ w Bydgoszczy" na podstawie stosunku pracy, chyba że nie zachodzi konflikt interesów lub podwójne finansowanie.
2. Nie jestem osobą/podmiotem powiązanym z Zamawiającym osobowo.
3. Nie jestem osobą/podmiotem podlegającym wykluczeniu z postępowania o udzielenie zamówienia na podstawie art. 7 ust. 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego z dnia 13.04.2022 r.
4. Oświadczam, że w związku z wystąpieniem okoliczności …… *(należy wskazać podstawę wykluczenia)* podjąłem następujące środki naprawcze: ……
5. Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

……
podpis osoby reprezentującej Wykonawcę

Załącznik nr 4
wzór

UMOWA nr ……
zawarta w formie elektronicznej

Strony umowy:
Szpitalem Klinicznym im. dr. Emila Warmińskiego Politechniki Bydgoskiej - SPZOZ w Bydgoszczy z siedzibą w Bydgoszczy (85-826), przy ul. Szpitalnej 19, wpisanym do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej prowadzonego przez Sąd Rejonowy w Bydgoszczy, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000057250, NIP: 953-22-93-970, REGON: 092354746, zwanym dalej **Zamawiającym,** w imieniu którego działa:

…… – ……..

a

…… z siedzibą w …….. (…..-…..), przy ul. ……., wpisaną do Krajowego Rejestru Sądowego pod numerem KRS …… prowadzonego przez Sąd Rejonowy w ……., ……. Wydział Gospodarczy Krajowego Rejestru Sądowego, NIP: ……., REGON: ……., zwaną dalej **Wykonawcą**, w imieniu której działa:

…… – ……..

Niniejsza umowa stanowi realizację zadania współfinansowanego w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (KPO), Komponent D „Efektywność, dostępność i jakość systemu ochrony zdrowia", Inwestycja D1.1.2 „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia", Tytuł Przedsięwzięcia: Transformacja cyfrowa Szpitala Klinicznego im. dr. Emila Warmińskiego Politechniki Bydgoskiej - SPZOZ w Bydgoszczy.

§ 1
Przedmiot zamówienia

1. W wyniku przeprowadzonego postępowania o udzielenie zamówienia publicznego prowadzonego na podstawie art. 2 ust. 1 pkt 1 ustawy Prawo zamówień Publicznych pn. ***„Aktualizacja polityk bezpieczeństwa wraz z audytem końcowym”***, Zamawiający wybrał ofertę złożoną przez Wykonawcę.
2. Na mocy niniejszej umowy Wykonawca zobowiązuje się do realizacji na rzecz Zamawiającego usług, których zakres i wielkość zostały określone w Opisie Przedmiotu Zamówienia (dalej: „OPZ”) oraz w ofercie Wykonawcy, stanowiącej załącznik nr 5 do umowy, zwanych dalej „Audytem” lub „Usługami”.

§ 2
Terminy i warunki świadczenia Usług

1. Strony ustalają, że Usługi będące przedmiotem niniejszej umowy zostaną zrealizowane w terminie **do 10.07.2026 r.** przy czym w pierwszej kolejności należy opracować dokumentację, a następnie przeprowadzić audyt.
2. Wykonawca zobowiązuje się przestrzegania przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz innych przepisów dotyczących ochrony danych osobowych obowiązujących w Polsce. Wykonawca zawrze z Zamawiającym odrębną umowę powierzenia przetwarzania danych osobowych, regulującą szczegółowo problematykę przetwarzania danych osobowych w relacjach między stronami. Umowa powierzenia przetwarzania danych osobowych stanowi załącznik nr 4 do niniejszej umowy. Wykonawca przyjmuje do wiadomości, że zawarcie umowy powierzenia przetwarzania danych osobowych jest warunkiem rozpoczęcia realizacji Usług.
3. Niezwłocznie po zakończeniu realizacji Usług dostarczy Zamawiającemu niezbędną dokumentację potwierdzającej przeprowadzone czynności oraz sporządzi protokół odbioru Usługi i przedstawi go do podpisu Zamawiającemu.
4. Wykonawca zobowiązany będzie w terminie do 2 miesięcy od dnia zakończenia audytu do jednorazowej aktualizacji wewnętrznych polityk oraz procedur bezpieczeństwa z uwzględnieniem potrzeb i uwag Zamawiającego.

§ 3
Wynagrodzenie

1. Wykonawca za należyte wykonanie umowy otrzyma wynagrodzenie w wysokości …….…… zł (słownie: ……) brutto.
2. Wynagrodzenie wskazane w § 3 ust. 1 wyczerpuje całość roszczeń Wykonawcy z tytułu wykonania niniejszej umowy.
3. Z momentem dostarczenia opracowań powstałych w wyniku realizacji Usług, Wykonawca złoży Zamawiającemu pisemne oświadczenie wskazujące czy dostarczone opracowania:
   1) powstały w ramach realizacji zamówienia objętego niniejszą umową i w wyniku działań sfinansowanych bądź współfinansowanych z wynagrodzenia przewidzianego umową;
   2) nie powstały w ramach działań sfinansowanych bądź współfinansowanych z wynagrodzenia przewidzianego Umową.
4. Jeśli opracowane materiały będę kwalifikowały się jako utwór w rozumieniu przepisów ustawy o prawie autorskim i prawach pokrewnych, w dalszej części umowy określane jako „Utwór" bądź zbiorczo „Utwory",
   1) Wykonawca gwarantuje i zapewni, że:
      a) w dacie ich wydania będzie mu przysługiwała całość majątkowych praw autorskich do Utworów;
      b) Utwory będą wolne od jakichkolwiek obciążeń i wad prawnych, a korzystanie z nich nie będzie naruszało praw osób trzecich.

2) Wykonawca z chwilą otrzymania wynagrodzenia bez konieczności składania w tym przedmiocie żadnych dodatkowych oświadczeń przenosi na Zamawiającego majątkowe prawa autorskie do Utworów na następujących polach eksploatacji:
   a) utrwalanie i zwielokrotnianie utworu lub jego części dowolną techniką, w szczególności wytwarzanie dodatkowych egzemplarzy (we wszystkich dostępnych technikach, włączając w to technikę drukarską, reprograficzną, zapisu magnetycznego oraz cyfrową);
   b) wprowadzenie i utrzymywanie w pamięci komputera lub w innym nośniku elektronicznym, do sieci wewnętrznych, do sieci Internet;
   c) wprowadzanie do obrotu oryginału utworu lub jego części albo egzemplarzy, na których utwór lub jego cześć zostały utrwalone, użyczania, najmu lub dzierżawy oryginału albo egzemplarzy;
   d) rozpowszechnianie Utworów lub jego części, w tym publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie, a także publiczne udostępnianie w taki sposób, aby każdy mógł mieć do nich dostęp w czasie i miejscu przez siebie wybranym;
   e) korzystanie w ramach działalność naukowej, dydaktycznej i gospodarczej prowadzonej przez Zamawiającego.
3) Wykonawca z chwilą wskazaną w pkt 2 powyżej (zapłata wynagrodzenia) udziela Zamawiającemu nieograniczonego czasowo i nieodwołalnego zezwolenia na wykonywanie autorskich praw zależnych do Utworów tj. na wykonywanie, rozporządzanie i korzystanie z opracowań Utworów na ww. polach eksploatacji wraz z prawem do udzielania takich zezwoleń osobom trzecim. W ramach tych uprawnień Zamawiający ma prawo do dowolnego wykorzystywania całości lub swobodnie wybranych fragmentów Utworu oraz ich dowolnego modyfikowania.
4) Wykonawca z chwilą wskazaną w pkt 2 powyżej (zapłata wynagrodzenia) zobowiązuje się do niewykonywania osobistych praw autorskich wynikających z art. 16 pkt 2, 3, 4 i 5, art. 49 ust. 2, art. 58 ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych oraz prawa do decydowaniu o wycofaniu utworu z obiegu, służących mu względem Utworów oraz do zapewnienia, iż tego rodzaju działania nie będą wykonywane przez osoby, którym służą prawa autorskie osobiste do Utworu, gdyby te prawa służyły osobom innym niż Wykonawca. Zobowiązanie wskazane w zdaniu pierwszym niniejszego ustępu ma charakter nieograniczony czasowo, nieodwołany i nie podlega wypowiedzeniu.
5) Wykonawca akceptuje fakt, że po zakończeniu realizacji umowy Utwory mogą zostać udostępnione przez Zamawiającego w domenie publicznej (w szczególności za pomocą sieci Internet) do korzystania na warunkach licencji otwartych typu „Creative Commons".

5. Co do przypadków o jakich mowa w ust. 4 pkt 2, jeśli opracowane materiały będę kwalifikowały się jako utwór w rozumieniu przepisów ustawy o prawie autorskim i prawach pokrewnych Wykonawca udziela Zamawiającemu licencji na okres 20 lat uprawniającej

Zamawiającego do wykorzystywania ich w ramach wewnętrznej działalności prowadzonej przez Zamawiającego.

6. Rozliczenia pomiędzy Zamawiającym a Wykonawcą będą się odbywały na podstawie faktury VAT dostarczonej po realizacji wszystkich Usług objętych przedmiotem zamówienia.
7. Zamawiający dokona zapłaty wynagrodzenia w terminie do 30 dni licząc od dnia doręczenia Zamawiającemu prawidłowo wystawionej faktury VAT, sporządzonej po podpisaniu przez Zamawiającego protokołu odbioru. Podstawą wystawienia faktury będzie obustronnie podpisany protokół. Za datę dokonania zapłaty przyjmuje się datę obciążenia rachunku bankowego Zamawiającego.
8. Wykonawca zobowiązuje się do ustalenia treści faktury z Zamawiającym przed jej wystawieniem z uwagi na finansowanie Przedmiotu Umowy ze źródeł zewnętrznych.
9. Faktury powinny być doręczone Zamawiającemu nie później niż 1 dzień roboczy od należytego wykonania Przedmiotu Umowy potwierdzonego podpisanym protokołem.
10. Wszelkie faktury będą wystawiane wyłącznie za pośrednictwem KSeF. Za datę doręczenia faktury przyjmuje się datę nadania jej numeru w KSeF.
11. Dopuszcza się przesyłanie załączników do faktur poprzez powiązanie z fakturą w KSeF tzw. KSeF/ID lub przesyłanie ich drogą mailową na adres faktury@szpital.pbs.edu.pl lub w innej formie i dostarczone nie później niż przesłana faktura za pośrednictwem KSeF.

§ 4

Rozwiązanie umowy

1. Strony zgodnie ustalają, że terminowa realizacja zamówienia ma dla Zamawiającego kluczowe znaczenie, wobec czego Wykonawca akceptuje wartość ustalonych kar umownych za zwłokę w wykonaniu zobowiązania jak również za rozwiązanie umowy.
2. Zamawiający ma prawo rozwiązać niniejszą umowę w trybie natychmiastowym, jeżeli:
   1) Wykonawca uchybił ustalonemu lub wyznaczonemu terminowi realizacji usług lub nie zapewnił odpowiedniej kadry celem ich prowadzenia;
   2) Wykonawca pomimo uprzedniego wezwania go przez Zamawiającego do prawidłowej realizacji umowy nie wykonuje obowiązków, o których mowa w § 2.
3. Oświadczenie o rozwiązaniu umowy wymaga zachowania formy pisemnej pod rygorem jego nieważności.

§ 5

Reprezentanci

1. Strony wskazują następujące osoby jako upoważnione do kontaktów w sprawach związanych z realizacją umowy oraz ich adresy poczty elektronicznej:
   1) ze strony Zamawiającego – ……,
   2) ze strony Wykonawcy – ……,
2. Zmiany wyznaczonych osób będą zgłaszane na podany powyżej adres e-mail. Zmiany te nie wymagają sporządzania aneksu.

3. Wyżej wskazane osoby wyznaczone zostały do kontaktów o charakterze roboczym i technicznym, nie są one umocowane do składania w imieniu Stron oświadczeń woli, w szczególności zaś do składania oświadczeń rodzących lub mogących rodzić zobowiązania finansowe, co nie wyłącza istnienia takiego umocowania wynikającego ze stosunków pozaumownych łączących daną osobę z jedną ze Stron.
4. Strony ustalają, że wszelkie istotne ustalenia, informacje i oświadczenia związane z realizacją umowy będą czynione i przekazywane wyłącznie w formie pisemnej lub mailowej. Wszelkie istotne ustalenia, informacje lub oświadczenia poczynione lub przekazane w formie telefonicznej lub ustnej uważa się za niewiążące/niebyłe, jeśli nie zostaną następnie potwierdzone przez obie Strony mailowo lub w formie pisemnej co do ich treści i daty przekazania.

§ 6
Kary umowne

1. Wykonawca zapłaci Zamawiającemu kary umowne w następujących okolicznościach:
   1) za przekroczenie terminu określonego w § 2 ust. 1 umowy z winy Wykonawcy (zwłokę) - w wysokości 1% wartości całkowitego wynagrodzenia Wykonawcy brutto, za każdy rozpoczęty dzień zwłoki, jednak w wysokości nie większej niż 30% tego wynagrodzenia;
   2) w przypadku nienależytego wykonania umowy, tj. stwierdzenia, że usługi były świadczone niezgodnie z zawartą umową, zaproszeniem do składania ofert lub złożoną ofertą – Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 5% wynagrodzenia wskazanego w § 3 ust. 1 umowy, za każdy stwierdzony przypadek. Przez sytuacje takie Strony rozumieją w szczególności następujące przypadki: brak zapewnienia odpowiedniej kadry celem realizacji Usług oraz brak ich realizacji w wymaganym zakresie;
   3) z tytułu rozwiązania umowy przez Zamawiającego z przyczyn za jakie odpowiedzialność ponosi Wykonawca lub z tytułu rozwiązania umowy przez Wykonawcę z przyczyn niezależnych od Zamawiającego, w wysokości 20% wartości całkowitego wynagrodzenia Wykonawcy brutto;
   4) za brak usunięcia uchybień w realizacji Umowy, do usunięcia których Zamawiający wezwał Wykonawcę na piśmie wyznaczając termin, 3% wartości całkowitego wynagrodzenia Wykonawcy brutto, za każdy taki stwierdzony przypadek.
2. Łączna maksymalna wysokość kar umownych nie może przekroczyć 30% wartości całkowitego wynagrodzenia Wykonawcy brutto.
3. Zamawiający zastrzega sobie prawo potrącania wszelkich kar umownych zastrzeżonych w Umowie z wynagrodzenia Wykonawcy, choćby nie było ono wymagalne, na co Wykonawca wyraża zgodę.
4. Uiszczenie kary umownej nie zwalnia Wykonawcy z realizacji obowiązków wynikających z niniejszej umowy.
5. Strony zastrzegają Zamawiającemu prawo dochodzenia odszkodowania przewyższającego wysokość zastrzeżonych kar na zasadach ogólnych. W przypadku wyrządzenia szkody przez

działania
lub zaniechania, na okoliczność wystąpienia których nie zastrzeżono prawa do naliczenia kar umownych, Strony zachowują prawo do dochodzenia odszkodowania na zasadach ogólnych.

§ 7
Zmiany Umowy

1. Wszelkie zmiany umowy, pod rygorem nieważności, mogą być dokonywane, wyłącznie za zgodą obu Stron, w formie pisemnej.

§ 8
Dostępność

1. Zamawiający działając na podstawie art. 4 ust. 3 ustawy z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz. U. z 2024, poz. 1411) określa, że w przypadku udziału w projekcie osób niepełnosprawnych, Wykonawca musi zapewnić im dostęp do udziału w Usługach oraz dostosować sposób ich prowadzenia oraz opracowane materiały do ich potrzeb.

§ 9
Postanowienia końcowe

1. W sprawach nieokreślonych w Umowie, mają zastosowanie postanowienia zaproszenia do składania ofert oraz przepisy prawa polskiego, w szczególności przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny.
2. Spory mogące wyniknąć z tej Umowy będzie rozpoznawał sąd powszechny właściwy dla siedziby Zamawiającego.
3. Wykonawca nie może przenieść swoich wierzytelności wynikających z niniejszej Umowy na podmiot trzeci bez uprzedniej pisemnej zgody Zamawiającego.
4. Wykonawca zobowiązuje się do niedokonywania przekazu świadczenia Zamawiającego (w rozumieniu art. 921^1-921^5 Kodeksu cywilnego), w całości lub w części, należnego na podstawie niniejszej Umowy.
5. Wykonawca zobowiązuje się do niezawierania umowy poręczenia przez osoby trzecie za długi Zamawiającego należne na podstawie niniejszej Umowy (w rozumieniu art. 876 - 887 Kodeksu cywilnego).
6. Wykonawca zobowiązuje się do nieudzielania jakiegokolwiek pełnomocnictwa ani upoważnienia do dochodzenia wierzytelności wynikających lub związanych z realizacją niniejszej Umowy, na drodze sądowej lub pozasądowej, za wyjątkiem pełnomocnictwa procesowego dla radcy prawnego lub adwokata.
7. Niniejsza Umowa została sporządzona w formie elektronicznej i udostępniona każdej ze Stron. Datą zawarcia Umowy jest data złożenia podpisu przez ostatnią ze Stron.
8. Ilekroć w toku realizacji Umowy Wykonawca popadnie w opóźnienie, jest zobowiązany niezwłocznie, nie później niż w ciągu 3 dni, przekazać Zamawiającemu szczegółowe

wyjaśnienia co do przyczyn stanu opóźnienia, oraz przedstawić stosowne dowody celem wyjaśnienia, że opóźnienie wynika z przyczyn niezawinionych przez Wykonawcę. W przypadku przedłożenia w terminie wyjaśnień, Zamawiający dokona klasyfikacji stanu opóźnienia z ich uwzględnieniem. W przypadku braku złożenia szczegółowych wyjaśnień wraz z właściwymi dowodami, Zamawiający ma prawo przyjąć, że opóźnienie jest stanem zawinionym przez Wykonawcę. Wykonawca odpowiada względem Zamawiającego za szkodę spowodowaną niewywiązaniem się z wyżej opisanych obowiązków, w szczególności wynikającą z podjęcia przez Zamawiającego określonych decyzji (np. o odstąpieniu od Umowy, o nałożeniu kar umownych, o wystąpieniu z powództwem przeciwko Wykonawcy).

9. Zgodnie z art. 4c ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych, Wykonawca oświadcza, że jest/nie jest dużym przedsiębiorcą w rozumieniu art. 4 pkt 6 tej ustawy.
10. Wykonawca zobowiązany jest do zawarcia z Zamawiającym umowy powierzenia przetwarzania danych osobowych, której wzór stanowi załącznik nr 4 do Umowy w terminie do 5 dni kalendarzowych od dnia zawarcia Umowy.

Załącznikami stanowiącymi integralną część niniejszej Umowy są:

1) Zał. nr 1 – wzór protokołu odbioru;
2) Zał. nr 2 - Zasady środowiskowe dla firm zewnętrznych;
3) Zał. nr 3 - lista podwykonawców / dalszych podwykonawców;
4) Zał. nr 4 - umowa powierzenia przetwarzania danych osobowych;
5) Zał. nr 5 - oferta Wykonawcy;
6) Zał. nr 6 – opis przedmiotu zamówienia – zaproszenie do składania ofert.

Wykonawca **Zamawiający**

Załącznik nr 1 do Umowy

Protokół odbioru

Sporządzony ……. w Bydgoszczy pomiędzy:
Szpitalem Klinicznym im. dr. Emila Warmińskiego Politechniki Bydgoskiej – SPZOZ w Bydgoszczy, ul. Szpitalna 19, 85-826 Bydgoszcz – **Zamawiającym**

a
_____ - Wykonawcą

W dniu …… r. Komisja w składzie:

……

……..

……..

oraz przy udziale przedstawiciela Wykonawcy:

……..

……..

stwierdza, co następuje:

……

……

……

……

Na tym protokół zakończono. Protokół sporządzono w dwóch jednobrzmiących egzemplarzach, w tym jeden dla Zamawiającego, jeden dla Wykonawcy.

WYKONAWCA **ZAMAWIAJĄCY**

Załącznik nr 2 do Umowy

	Szpital Kliniczny im. dr. Emila Warmińskiego Politechniki Bydgoskiej - SPZOZ w Bydgoszczy	**PR20_PŚ3_z2_ w3**
	ZASADY ŚRODOWISKOWE i BHP DLA FIRM ZEWNĘTRZNYCH / WYKONAWCÓW	

1. Podmiot zewnętrzny związany umową ze Szpitalem, działający na terenie Szpitala zobowiązany jest do przestrzegania wymagań określonych w systemie zarządzania środowiskowego wg norm ISO 14001 oraz w systemie zarządzania bezpieczeństwem i higieną pracy ISO 45001.
2. Podmiot zewnętrzny związany umową ze Szpitalem zobowiązany jest w szczególności do:
   a) realizacji zadania w sposób najmniej uciążliwy dla środowiska w tym racjonalnego korzystania z wody, energii elektrycznej, zapobiegania zanieczyszczeniom oraz ochrony terenów zielonych;
   b) właściwej gospodarki odpadami:
      - minimalizowania ilości powstających odpadów,
      - gromadzenia wytworzonych odpadów w wyznaczonych, oznakowanych i zabezpieczonych miejscach,
      - usuwania odpadów z miejsca ich powstania w miarę możliwości na bieżąco,
      - prowadzenia segregacji odpadów w miejscu ich powstawania,
      - niedopuszczania do mieszania odpadów niebezpiecznych z innymi niż niebezpieczne,
      - stosowania się do aktualnych wymagań prawnych (m. in. posiadania, o ile są wymagane, stosownych decyzji w przedmiotowym zakresie);
      - wywożenia i unieszkodliwienia powstałych na skutek świadczenia usług odpadów na własny koszt i odpowiedzialność,
      - posiadania odpowiedniej dokumentacji potwierdzającej unieszkodliwienie wytworzonych odpadów,
      - wytwórcą odpadów powstających w wyniku świadczenia usług jest podmiot, który świadczy usługę, chyba że umowa o świadczenie usługi stanowi inaczej;
   c) realizacji następujących działań w zakresie bhp i ppoż:
      - podmiot zewnętrzny ponosi pełną odpowiedzialność za przestrzeganie obowiązujących na terenie Szpitala przepisów i zasad bhp i ppoż. oraz za stosowanie bezpiecznych metod pracy,
      - firma zewnętrzna jest obowiązana do zapewnienia bezpieczeństwa własnym pracownikom oraz wyposażenia ich w niezbędne środki ochrony indywidualnej i zbiorowej,

- firma zewnętrzna jest obowiązana do przedstawienia na życzenie Szpitala oświadczenia o ważności badań lekarskich swoich pracowników (w tym oświadczenia o dopuszczeniu danego pracownika do prac na wysokości jeżeli jest to konieczne),
- w przypadku gdy pracownicy firmy zewnętrznej wykonują na terenie Szpitala usługi remontowo-budowlane przed przystąpieniem do prac powinni oni zgłosić się do specjalisty ds. bhp w celu odbycia szkolenia.

3. Na terenie Szpitala bezwzględnie zabrania się:
   - wwożenia na teren Szpitala jakichkolwiek odpadów,
   - składowania substancji mogących zanieczyścić powietrze atmosferyczne, wodę i glebę, w przypadku gdy substancje te służą do wykonywania usług, szczegóły ich stosowania, zabezpieczania i składowania należy ustalić z Działem Eksploatacyjno-Technicznym lub Specjalistą ds. ochrony środowiska,
   - spalania odpadów,
   - wrzucania wytworzonych odpadów do kontenerów i pojemników Zleceniodawcy,
   - składowania odpadów bezpośrednio na ziemi, które mogłyby spowodować skażenie gruntu, wody, powietrza,
   - wylewania żrących, trujących oraz innych niebezpiecznych substancji, płynów do kanalizacji lub bezpośrednio do ziemi;
   - mycia pojazdów i sprzętu,
   - przechowywania zapasów paliwa i tankowania pojazdów,
   - palenia tytoniu i używania otwartego ognia.
4. W zakresie mediów energetycznych i wody wykorzystanie ich jest możliwe wyłącznie w porozumieniu i po uzgodnieniach z uprawnionym przedstawicielem podmiotu zewnętrznego z Działem Eksploatacyjno-Technicznym Szpitala.
5. W przypadku zniszczenia trawników, zadrzewień podmiot zewnętrzny związany umową ze Szpitalem zobowiązany jest do przywrócenia ich stanu pierwotnego.
6. W miejscu świadczenia usług należy utrzymywać ład i porządek.
7. W przypadku wystąpienia sytuacji niebezpiecznej lub awarii środowiskowej, podmiot zewnętrzny związany umową ze Szpitalem zobowiązany jest do przerwania pracy i natychmiastowego podjęcia działań minimalizujących skażenie środowiska oraz poinformowania o zaistniałym zdarzeniu osobę nadzorującą wykonanie umowy z ramienia Szpitala oraz Specjalistę ds. ochrony środowiska i Specjalistę ds. bhp i ppoż.
8. Przedstawiciel podmiotu zewnętrznego zobowiązany jest przeprowadzić szkolenie wśród podległych pracowników wykonujących usługę w zakresie wymienionych powyżej zasad środowiskowych.
9. Podmiot zewnętrzny wyraża zgodę na przeprowadzenie kontroli postępowania w zakresie zgodności z przyjętymi zasadami przez Specjalistę ds. bhp i ppoż. oraz Specjalistę ds. ochrony środowiska.
10. W sytuacjach wątpliwych i nieokreślonych w powyższych zasadach należy zwracać się do Specjalisty ds. ochrony środowiska nr tel. 52/ 37 09 140 lub Specjalisty ds. bhp i ppoż. nr tel. 52/ 37 09 133.

Załącznik nr 3 do Umowy

Lista podwykonawców / dalszych podwykonawców

Zakres podwykonawstwa	Podwykonawca / Dalszy Podwykonawca (nazwa i NIP)	Dane kontaktowe Podwykonawcy / Dalszego Podwykonawcy

Załącznik nr 4 do Umowy

Umowa powierzenia przetwarzania danych osobowych

zawarta w formie elektronicznej pomiędzy

(zwana dalej „Umową powierzenia")

Szpitalem Klinicznym im. dr. E. Warmińskiego Politechniki Bydgoskiej – SPZOZ w Bydgoszczy
(85 – 826) przy ul. Szpitalnej 19, wpisanym do Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy w Bydgoszczy, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000057250, NIP: 953-22-93-970, REGON: 092354746, zwanym w dalszej części Umowy powierzenia **„Administratorem danych" lub „Administratorem",**
reprezentowanym przez:
……

oraz

……
zwanym w dalszej części Umowy „podmiotem przetwarzającym"

§ 1

[Powierzenie przetwarzania danych osobowych]

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 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) (Dz. Urz. UE L Nr 119 z 4.5.2016 r. s. 1–88 ze zm.; dalej: RODO) dane osobowe do przetwarzania, na zasadach i w celu realizacji Umowy Głównej.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową powierzenia, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, że stosuje środki bezpieczeństwa spełniające wymogi RODO.
4. Podmiot przetwarzający oświadcza, że przetwarza dane w zgodzie z art. 34 ust. 5 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206).

§ 2

[Zakres i cel przetwarzania danych]

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie Umowy Głównej **dane zwykłe pracowników Administratora w postaci: imię i nazwisko.**
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji **Umowy nr …… .**

§ 3

[Obowiązki podmiotu przetwarzającego]

1. Podmiot przetwarzający zobowiązuje się przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 RODO.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji Umowy Głównej.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy (o której mowa w art. 28 ust. 3 pkt b RODO) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji Umowy Głównej, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32–36 RODO.

§ 4

[Prawo kontroli]

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) RODO ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy powierzenia.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 48 godzin jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.

§ 5

[Dalsze powierzenie danych do przetwarzania]

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą Umową powierzenia do dalszego przetwarzania podwykonawcom jedynie w celu wykonania Umowy Głównej po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych, chyba że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot

przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, powinien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie powierzenia.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

[Odpowiedzialność Podmiotu przetwarzającego]

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy powierzenia, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w Umowie powierzenia, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§ 7

[Czas obowiązywania Umowy powierzenia]

1. Niniejsza Umowa powierzenia obowiązuje od dnia jej zawarcia przez czas trwania Umowy Głównej.

§ 8

[Rozwiązanie Umowy powierzenia]

Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:

1) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
2) przetwarza dane osobowe w sposób niezgodny z Umową powierzenia;
3) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§ 9

[Zasady zachowania poufności]

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji,

danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").

2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy Głównej, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy Głównej.

§ 10

[Postanowienia końcowe]

1. Niniejsza Umowa powierzenia została sporządzona w formie elektronicznej i udostępniona każdej ze Stron. Datą zawarcia Umowy powierzenia jest data złożenia podpisu przez ostatnią ze Stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy ustawy z 23.04.1964 r. – Kodeks cywilny (t.j. Dz.U. z 2025 r. poz. 1071 ze zm.) oraz RODO.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy powierzenia będzie sąd miejscowo właściwy dla Administratora danych.

…… ……

Podmiot przetwarzający *Administrator danych*

załącznik nr 3 do zaproszenia

Audyt końcowy w obszarze cyberbezpieczeństwa

Audyt powinien obejmować przynajmniej obszary, w których przetwarzane są dane osobowe wrażliwe, w tym kluczowe systemy informacji medycznej oraz infrastrukturę urządzeń medycznych (aparatura medyczna wraz z systemami je obsługującymi). Audyt powinien obejmować niezbędną infrastrukturę teleinformatyczną podmiotu, w tym przynajmniej bezpieczeństwo takich elementów jak:

- Kanały komunikacji jak np. poczta
- Sieciowe urządzenia brzegowe wraz z zasadami segmentacji oraz przepływów
- Kontrolery domeny
- Platforma wirtualizacyjna
- System zarządzania kopiami zapasowymi
- Poprawność konfiguracji stacji roboczych oraz serwerów
- Sposoby uwierzytelniania się użytkowników

Zespół audytujący: co najmniej dwóch audytorów posiadających certyfikaty określone w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. (Dz.U. poz. 1999) w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu lub co najmniej dwóch audytorów posiadających co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych lub jednostka oceniająca zgodność, akredytowana zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854 z późn.zm.), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych.

Ankieta weryfikacji dojrzałości pod kątem cyberbezpieczeństwa

1) System kopii zapasowych

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożony system tworzy odmiejscowione kopie zapasowe. System posiada aktualne wsparcie producenta oraz wykonuje kopie kluczowych systemów podmiotu.		**Tak**
2.	Infrastruktura systemu backupu jest odseparowana od systemu produkcyjnego		**Tak**
3.	Przeprowadzono testy odtworzenia systemu i potwierdzono skuteczność/poprawność odtworzenia		**Tak**
4.	Podmiot posiada dokumentację powdrożeniową systemu backupu.		**Tak**
5.	Administratorzy systemu backupu podmiotu odbyli instruktaż z obsługi systemu kopii zapasowych.		**Tak**
6.	Wdrożono procedury backupowe oraz odtworzeniowe i procedury te są stosowane.		**Nie**
7.	Tworzone są i weryfikowane raporty z cyklicznego wykonywania odmiejscowionej kopii zapasowej.		**Nie**

8.	Podmiot cyklicznie odtwarza dane z kopii zapasowych w celu weryfikacji poprawności. Odtworzenia testowe potwierdzone są protokołem.		**Nie**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Zestawienie wszystkich kluczowych i pomocniczych systemów objętych systemem kopii zapasowych – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.
- Dokument zawierający wymagania dotyczące częstotliwości wykonywania kopii zapasowych – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.
- Kompletna dokumentacja wdrożonego rozwiązania systemu kopii zapasowych w szczególności zestaw procedur wykonywania, odtworzenia (w tym cyklicznych testów), zabezpieczenia odmiejscowionej kopii, monitoringu i weryfikacji poprawności działania systemu, zarządzania uprawnieniami i dostępem do systemu – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.
- Raport z testów funkcjonalnych i niefunkcjonalnych działania systemu backupu – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.
- Potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi systemu kopii zapasowej – w zakresie usług szkoleniowych.
- Wyniki testu potwierdzającego skuteczności wprowadzonych zabezpieczeń i potwierdzającego zgodność konfiguracji z dokumentacją – dla usług testów bezpieczeństwa.
- Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych

2) Zapory sieciowe

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożono moduł ochrony przed złośliwym oprogramowaniem dla ruchu z/do Internetu, posiadający aktualne wsparcie.		**Tak**
2.	Wdrożono i włączono moduł IPS/IDS przynajmniej dla ruchu z/do Internetu, posiadający aktualne wsparcie.		**Tak**
3.	Wdrożono i włączono moduły filtrowania zawartości oraz reguły filtrowania po kategorii treści.		**Tak**
4	Na brzegu sieci zainstalowany Firewall, a sama sieć podzielona jest na podsieci.		**Tak**
5.	Kluczowe aplikacje/systemy, w szczególności dostępne publicznie chronione są za pomocą firewalla aplikacyjnego (WAF) z włączonymi modułami ochrony aplikacji, ochrony DoS/DDoS.		**Nie**
6.	Pliki pobierane z sieci Internet podlegają analizie w izolowanych środowiskach typu Sandbox.		**Nie**
7.	Domyślne hasła przekazane przy odbiorze zostały zmienione i objęte procedurą zarządzania hasłami w organizacji.		**Tak**
8.	Nieużywane porty, usługi oraz konta zostały wyłączone.		**Tak**
9.	Dostęp do panelu zarządzania zaporą sieciowy został ograniczony jedynie dla wyznaczonych osób zgodnie z obowiązującą procedurą nadawania uprawnień oraz dostępny jest wyłącznie z wybranej podsieci.		**Tak**

10.	Wdrożona została procedura cyklicznego wykonywania kopii zapasowych konfiguracji urządzenia (lub po każdej zmianie reguł i wersji) .Procedura ta jest stosowana.		**Tak**
11.	Administratorzy posiadają kompetencje w postaci odbytego instruktażu stanowiskowego i/lub odbytych szkoleń z obsługi dedykowanego systemu Firewall.		**Tak**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Dokumentacja powykonawcza wdrożonych zapór sieciowych wraz z zabezpieczeniami – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.
- Wyniki testu potwierdzającego skuteczność wprowadzonych zabezpieczeń i potwierdzającego zgodność konfiguracji z dokumentacją – dla usług testów bezpieczeństwa.
- Potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi zainstalowanych zapór sieciowych – dla usług szkoleniowych.
- Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych.

3) Ochrona poczty e-mail

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożono mechanizmy ochrony poczty SPF, DMARC, DKIM.		**Tak**
2.	Wdrożono ochronę antyspam oraz ochronę przed złośliwym oprogramowaniem, z aktualnym wsparciem producenta i aktualnymi sygnaturami.		**Tak**
3.	Przeprowadzono testy wdrożonych mechanizmów ochrony poczty, które potwierdziły poprawne ich działanie.		**Tak**
4.	Wdrożono obowiązkowy drugi składnik uwierzytelniający (2FA) dla poczty dostępnej z sieci publicznej.		**Tak**
5.	Uwierzytelnianie do poczty dostępnej publicznie jest zgodne ze standardem FIDO2.		**Nie**
6.	Wdrożono zasady bezpiecznego wykorzystania poczty w organizacji.		**Nie**
7.	Wiadomości przychodzące z zewnątrz oznaczane są dedykowanym banerem.		**Nie**
8.	Administratorzy posiadają kompetencje w postaci odbytego instruktażu stanowiskowego z obsługi dedykowanego systemu lub usługi.		**Tak**
9.	Kopia bezpieczeństwa poczty jest regularnie wykonywana.		**Tak**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Opis sposobu ochrony poczty wraz z dokumentacją systemów ochrony poczty
- Protokół z testów, który opisuje wyniki testów wdrożonych polityk ochrony poczty w tym weryfikację mechanizmów (SPF, DMARC, DKIM) ochrony poczty elektronicznej przy pomocy portalu CERT Polska https://bezpiecznapoczta.cert.pl/
- Wynik testu potwierdzającego wdrożenie obowiązkowego drugiego składnika uwierzytelniającego (2FA) dla poczty elektronicznej dostępnej publicznie.
- Raport z wykonania backupu poczty elektronicznej wraz testowym odtworzeniem.
- Raport zawierający informacje o aktualizacji systemu pocztowego wraz z jego ochroną

4) Segmentacja sieci

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożono segmentację sieciową (na poziomie VLANów) zapewniającą odseparowanie sieci biurowej, systemów serwerowych, systemu kopii zapasowych, urządzeń medycznych, sieci gościnnej.		**Tak**
2.	Wdrożono reguły bezpieczeństwa pomiędzy segmentami sieci oparte na zasadzie minimalnego niezbędnego dostępu.		**Tak**
3.	Dokumentacja architektury sieciowej jest sporządzona i aktualizowana.		**Nie**
4.	Wszystkie podłączane do sieci urządzenia są identyfikowane, uwierzytelniane oraz autoryzowane.		**Nie**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Dokument zawierający wymagania dotyczące podziału sieci wraz ze sposobem implementacji – dla zakupu sprzętu, oprogramowania oraz usług wdrożeniowych.
- Dokumentacja sposobu identyfikowania, uwierzytelniania i autoryzacji urządzeń podłączanych do sieci – dla zakupu oprogramowania.
- Wynik weryfikacji zgodności konfiguracji z dokumentacją– dla zakupu sprzętu, oprogramowania oraz usług wdrożeniowych.
- Potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi zainstalowanych systemów ochrony sieciowej – dla usług szkoleniowych
- Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych.
- Wyniki testu potwierdzającego skuteczność wprowadzonych zabezpieczeń i potwierdzającego zgodność konfiguracji z dokumentacją – dla usług testów bezpieczeństwa.

5) Ochrona stacji roboczych oraz serwerów (rozwiązania klasy EDR)

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożono rozwiązanie ochrony przed złośliwym oprogramowaniem z aktualnym wsparciem producenta.		**Tak**
2.	Wdrożono rozwiązanie klasy EDR, obejmujące wszystkie wspierane przez producenta oprogramowania stacje robocze oraz serwery.		**Tak**

3.	Wdrożono rozwiązanie klasy XDR, obejmujące wszystkie wspierane przez producenta oprogramowania stacje robocze i serwery oraz zbierające i analizujące dane również z innych źródeł.		**Nie**
4.	Dla serwerów oraz stacji roboczych nieobjętych ochroną została wykonana analiza ryzyka.		**Tak**
5.	Osoby administrujące systemami ochrony stacji i serwerów posiadają odpowiednie kompetencje potwierdzone odbytym szkoleniem.		**Tak**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Dokumentacja powykonawcza wdrożonego rozwiązania, potwierdzająca zastosowanie polityk bezpieczeństwa oraz wdrożenie agentów rozwiązania na stacjach roboczych oraz serwerach – dla zakupu sprzętu i oprogramowania oraz usług wdrożeniowych.
- Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych.
- Potwierdzenie uczestnictwa na szkoleniach z zakresu obsługi systemu – dla usług szkoleniowych.

6) Zarządzanie podatnościami

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożono system automatycznego (sieciowego i/lub agentowego) skanowania i identyfikacji podatności.		**Nie**
2.	Skanowanie podatności obejmuje przynajmniej kluczowe stacje robocze, serwery oraz urządzenia sieciowe.		**Nie**
3.	Skanowanie podatności obejmuje proces uwierzytelnienia się do poziomu systemu operacyjnego skanowanego hostu.		**Nie**
4.	Skanowanie podatności obejmuje ocenę poprawności konfiguracji bezpieczeństwa skanowanego hostu.		**Nie**
5.	Ocena ryzyka podatności uwzględnia inne czynniki niż system klasyfikacji CVSS.		**Nie**
6.	Ustalono czasy reakcji na zidentyfikowane podatności.		**Nie**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Dokumentacja powykonawcza wdrożonego i uruchomionego systemu, wskazująca na obszary objęte skanowaniem podatności – dla zakupu oprogramowania lub zakupu wsparcia oraz usług wdrożeniowych.
- Potwierdzenie uczestnictwa w szkoleniach – dla usług szkoleniowych.
- Wyciąg z umowy obejmujący zakres usługi – dla usług utrzymaniowych.

7) System zarządzania bezpieczeństwem informacji

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wdrożono politykę zarządzania dostępem i uprawnieniami.		**Tak**

2.	Wdrożono politykę kryptografii z uwzględnieniem zalecanych dopuszczalnych protokołów szyfrowania.		**Tak**
3.	Wdrożono politykę zarządzania podatnościami		**Tak**
4.	Wdrożono politykę zarządzania ryzykiem z uwzględnieniem obszaru cyberbezpieczeństwa		**Tak**
5.	Wdrożono politykę logowania zdarzeń z uwzględnieniem aplikacji, sieci, serwerów, bramy brzegowej, kontrolerem domeny.		**Tak**
6.	Wdrożono politykę kopii bezpieczeństwa.		**Tak**
7.	Wdrożono politykę zarządzania incydentami bezpieczeństwa.		**Tak**
8.	Wdrożono politykę zarządzania ciągłością działania.		**Tak**
9.	Wdrożono politykę ochrony danych osobowych z uwzględnieniem przetwarzania danych medycznych		**Tak**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Oświadczenie osoby uprawnionej do reprezentacji podmiotu, że kierownictwo ustanowiło lub zmodyfikowało System Zarządzania Bezpieczeństwem Informacji, oraz że zostały alokowane zasoby ludzkie i finansowe, niezbędne do jej realizacji, monitorowania i okresowych przeglądów.
- Lista opracowanej dokumentacji wraz z opisem
- Potwierdzenie uczestnictwa w szkoleniach – dla usług szkoleniowych

8) Szkolenia z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny)

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Odbycie szkolenia przez kadrę kierowniczą, w okresie ostatniego roku, minimum w zakresie: • Podstaw prawnych w obszarze cyberbezpieczeństwa • Typów ataków • Reagowania na incydenty • Wykonywania badań bezpieczeństwa • Roli kadry zarządzającej w procesach bezpieczeństwa		**Tak**
2.	Odbycie szkolenia przez kadrę biurową i medyczną – min. 75% pracowników pracujących na systemach informatycznych szpitala, w okresie ostatniego roku, minimum w zakresie: • Podstawowych zasad cyberhigieny • Typów ataków wraz z przykładami • Reagowania na incydenty		**Tak**

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Konspekt programu szkoleń
- Potwierdzenie uczestnictwa w szkoleniach co najmniej 75% pracowników szpitala, pracujących na stacjach roboczych – oświadczenie dyrektora szpitala

9) Usługi zarządzane bezpieczeństwa

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Systemy teleinformatyczne jak i infrastruktura teleinformatyczna monitorowana jest całodobowa pod kątem bezpieczeństwa		Nie
2.	Przygotowano i przetestowano indywidualne procedury reagowania na incydenty bezpieczeństwa dla najbardziej powszechnych i najczęściej pojawiających się zdarzeń		Nie
3.	Utrzymywany jest centralny system klasy SIEM lub system centralnej kolekcji zdarzeń/logów gromadzący istotne z punktu widzenia zdarzenia bezpieczeństwa z infrastruktury teleinformatycznej oraz aplikacji i systemów		Nie
4.	Kluczowe aplikacje, systemy oraz infrastruktura teleinformatyczna testowana jest pod kątem bezpieczeństwa		Nie
5.	Ubezpieczenie od ryzyk cybernetycznych stosowane jest jako element uzupełniający zarządzania ryzykiem.		Nie

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Umowa o świadczenie usług Centrum Operacji Bezpieczeństwa – w zakresie usług SOC.
- Wykaz przygotowanych Scenariuszy Reakcji dla zidentyfikowanych zagrożeń – w zakresie usługi przygotowania i wdrożenia scenariuszy.
- Umowa o świadczenie usług udostępniania i zarządzania systemem SIEM – w zakresie tego systemu.
- Umowa o świadczenie usług testów bezpieczeństwa – w zakresie usług testów.

10) Uwierzytelnienie i autoryzacja do systemów

Lp.	Nazwa kryterium	Czy spełnione? (Tak / Nie)	Czy obligatoryjne?
1.	Wszystkie krytyczne systemy w organizacji wymagają użycia drugiego składnika uwierzytelniania lub uwierzytelniania bezhasłowego.		Nie
2.	Każda osoba w organizacji ma obowiązek korzystania z drugiego składnika uwierzytelniania lub uwierzytelniania bezhasłowego (jeżeli jest dostępny).		Nie
3.	W przypadku wykorzystywania systemu pojedynczego logowania dla dostępu do systemów i aplikacji, uwierzytelnienie użytkownika odbywa się z wykorzystaniem metod wieloskładnikowych lub uwierzytelniania bezhasłowego.		Nie
4.	Wyłączono możliwość używania SMS-ów jako metody uwierzytelniania.		Nie
5.	Uwierzytelnianie do krytycznych systemów i aplikacji w organizacji jest zgodne ze standardem FIDO2.		Nie
6.	Wszystkie połączenia zdalne wymagają wieloskładnikowego uwierzytelniania.		Nie
7.	Uwierzytelnianie użytkownika uwzględnia jego kontekst np. urządzenie z którego następuje logowanie.		Nie

Kryteria akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa:

- Dokumentacja powykonawcza wdrożonych rozwiązań uwierzytelniających wraz z zabezpieczeniami – dla zakupu urządzeń i oprogramowania oraz usług wdrożeniowych.
- Potwierdzenie uczestnictwa w szkoleniach – dla usług szkoleniowych.

Wskaźnik D21G.R2:

Zabezpieczenie przetwarzania elektronicznej dokumentacji medycznej potwierdzone audytem bezpieczeństwa

– jednostka miary: liczba, wartość docelowa: 1

Sposób pomiaru: monitorowanie wzrostu poziomu cyberbezpieczeństwa w stosunku do *Ankiety weryfikacji dojrzałości pod kątem cyberbezpieczeństwa*

Mechanizm weryfikacji: wykonanie audytu bezpieczeństwa zgodnie z wymaganiami określonymi w kryteriach akceptacji do oceny przy audycie końcowym w obszarze cyberbezpieczeństwa