Załącznik nr 6 Kwestionariusz i Oświadczenie Bezpieczeństwa IT.

Niniejszy dokument stanowi skonsolidowany załącznik do umowy na świadczenie usług, opracowany w celu zapewnienia zgodności z dyrektywą NIS2, ustawą o Krajowym Systemie Cyberbezpieczeństwa oraz RODO w sektorze ochrony zdrowia.

I. Dane Wykonawcy

- **Nazwa firmy:** .....
- **Osoba do kontaktu w sprawach bezpieczeństwa:** .....
- **Email/Telefon:** .....

II. Kwestionariusz Samooceny Bezpieczeństwa

Obszar	Wymaganie / Pytanie (Wymagania obligatoryjne - zaznaczono)	Status (Tak/Nie) / Opis, jeżeli Nie	Wymóg – niespełnienie może powodować odrzucenie oferty
Bezpieczeństwo Organizacyjne	Czy Wykonawca posiada wdrożony system zarządzania bezpieczeństwem informacji (np. ISO/IEC 27001)?		Nie jest wymagane
	Czy Wykonawca posiada spisaną i wdrożoną Politykę Bezpieczeństwa Informacji (PBI/SZBI) w tym wszystkie wymagane prawem rejestry, analizy ryzyka, plany zapewnienia ciągłości działania itp.?		Tak

Obszar	Wymaganie / Pytanie (Wymagania obligatoryjne - zaznaczono)	Status (Tak/Nie) / Opis, jeżeli Nie	Wymóg – niespełnienie może powodować odrzucenie oferty
	Czy pracownicy biorący udział w realizacji umowy przechodzą regularne szkolenia z cyberbezpieczeństwa?		Tak
	Czy Wykonawca posiada doświadczenie w świadczeniu usług związanych z powierzeniem przetwarzania danych? Jeśli tak, to jak długie? Prosimy o wykazanie doświadczenia w świadczeniu przedmiotowych usług (o ile to możliwe, wskazanie podmiotów, z którymi Wykonawca współpracował w ww. zakresie i czasie trwania współpracy).		Nie jest wymagane
	Czy Wykonawca wyznaczył Inspektora Ochrony Danych. Jeżeli tak prosimy o podanie danych kontaktowych.		Nie jest wymagane
	Czy stwierdzono prawomocną decyzją PUODO lub innego organu nadzorczego lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez		Nie jest podstawą odrzucenie oferty, jeżeli

Obszar	Wymaganie / Pytanie (Wymagania obligatoryjne - zaznaczono)	Status (Tak/Nie) / Opis, jeżeli Nie	Wymóg – niespełnienie może powodować odrzucenie oferty
	Wykonawcę (odnosi się to również do poprzednika prawnego Wykonawcy)?		Wykonawca wdrożył zalecane przez UODO środki bezpieczeństwa, które poprawiają zabezpieczenie danych osobowych
	Czy w chwili obecnej prowadzone jest wobec Wykonawcy, postępowanie przed PUODU? Proszę o podanie etapu postępowania.		Nie jest podstawą odrzucenia oferty, jednak Wykonawca zobowiązany jest do przedłożenia informacji w

Obszar	Wymaganie / Pytanie (Wymagania obligatoryjne - zaznaczono)	Status (Tak/Nie) / Opis, jeżeli Nie	Wymóg – niespełnienie może powodować odrzucenie oferty
			momencie zakończenia procedury o wyniku postępowania.
Bezpieczeństwo Techniczne	Czy dane medyczne i wrażliwe są szyfrowane w spoczynku i w transmisji (min. AES-256, TLS 1.2/1.3)?		Tak
Bezpieczeństwo Techniczne	Czy dostęp do systemów administracyjnych i medycznych jest zabezpieczony przez MFA?		Tak
Bezpieczeństwo Techniczne	Czy Wykonawca zapewnia regularne wykonywanie i testowanie kopii zapasowych (backup)?		Tak
Bezpieczeństwo Techniczne	Jaki jest maksymalny czas przywrócenia sprawności systemu (RTO)?		Nie dłuższy niż (24) godziny

Obszar	Wymaganie / Pytanie (Wymagania obligatoryjne - zaznaczono)	Status (Tak/Nie) / Opis, jeżeli Nie	Wymóg – niespełnienie może powodować odrzucenie oferty
Zgodność z NIS2 / Medycyna	Czy system zapewnia pełną rozliczalność działań personelu (audit logs)?		Tak
Zgodność z NIS2 / Medycyna	Czy Wykonawca gwarantuje, że dane nie są przetwarzane poza terytorium EOG bez zgody Zamawiającego?		Tak
Zgodność z NIS2 / Medycyna	Czy Wykonawca posiada procedurę raportowania incydentów w czasie nie dłuższym niż 24h?		Tak

III. Oświadczenie o Bezpieczeństwie Łańcucha Dostaw

Wykonawca niniejszym oświadcza, co następuje:

1. Dostarczane rozwiązania (sprzęt, oprogramowanie, usługi) nie zawierają komponentów pochodzących od dostawców uznanych przez organy państwowe RP za dostawców wysokiego ryzyka w rozumieniu ustawy o Krajowym Systemie Cyberbezpieczeństwa.
2. Wykonawca monitoruje bezpieczeństwo swoich poddostawców i gwarantuje, że stosują oni standardy bezpieczeństwa nie niższe niż określone w niniejszym dokumencie.
3. Oprogramowanie dostarczane w ramach umowy jest wolne od znanych podatności krytycznych w momencie wdrożenia, a Wykonawca zobowiązuje się do dostarczania aktualizacji bezpieczeństwa przez cały okres trwania umowy.
4. W przypadku wykrycia zagrożenia w łańcuchu dostaw, Wykonawca niezwłocznie (nie później niż w ciągu 12h) poinformuje o tym Zamawiającego.

5. Wszyscy pracownicy oraz podwykonawcy skierowani do realizacji zadań, zarówno w momencie rozpoczęcia prac, jak i w całym okresie obowiązywania umowy (w tym osoby dołączające do zespołu w przyszłości), spełniają wymóg niekaralności w zakresie przestępstw przeciwko ochronie informacji, przestępstw przeciwko wiarygodności dokumentów oraz przestępstw związanych z cyberbezpieczeństwem i mieniem.
6. Wykonawca zobowiązuje się do bieżącej weryfikacji braku wpisów w Krajowym Rejestrze Karnym (KRK) w odniesieniu do każdego pracownika kierowanego do wykonywania świadczeń przed jego dopuszczeniem do przetwarzania informacji lub dostępu do systemów IT Zamawiającego.
7. Wykonawca zobowiązuje się do niezwłocznego wycofania z realizacji zadań każdej osoby, w stosunku do której powziął informację o wszczęciu postępowania karnego w wyżej wymienionym zakresie lub wydaniu wyroku skazującego, a także do poinformowania o tym fakcie Zamawiającego.
8. Na każde wezwanie Zamawiającego Wykonawca niezwłocznie przedstawi stosowne oświadczenia lub zaświadczenia z KRK potwierdzające spełnienie powyższych wymogów przez wskazanych członków zespołu.

IV. Zobowiązania Końcowe

Wykonawca przyjmuje do wiadomości, że złożenie nieprawdziwych oświadczeń w powyższej ankiecie może stanowić podstawę do natychmiastowego wypowiedzenia umowy z winy Wykonawcy oraz naliczenia kar umownych.

.....
(Podpis Wykonawcy)