Załącznik nr 1 do zapytania - Opis przedmiotu zamówienia

DOTYCZY: **Świadczenia asysty technicznej nad posiadanym systemem do archiwizacji badań endoskopowych**

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA:

Przedmiotem zapytania jest:
Usługa asysty technicznej dla posiadanego przez Zamawiającego systemu informatycznego do archiwizacji badań endoskopowych na okres 24/36 miesięcy od daty podpisania umowy
Zamawiający informuje że posiada licencje na system do archiwizacji badań endoskopowych wraz z integracją, z systemem HIS oraz PACS–ENDOBASE Wersja 14.9
W ramach zawartej umowy Wykonawca zapewni:

1. Usługę asysty technicznej dla systemu obejmującego:
    - System do archiwizacji badań endoskopowych wraz z integracją, z systemem HIS oraz PACS–ENDOBASE Wersja 14.9 (zwanego dalej Systemem)
    - Sprzęt serwerowy – serwer na potrzeby Systemu
2. Usługa asysty technicznej będzie świadczona na rzecz jednostek organizacyjnych Zamawiającego i musi być świadczona w języku polskim .
3. Warunki, jakie muszą spełnić Wykonawcy uczestniczący w postępowaniu:
    - W przypadku świadczenia usługi asysty technicznej przez Wykonawcę niebędącego producentem oprogramowania, Wykonawca musi posiadać zaświadczenie producenta oprogramowania, że może świadczyć usługi asysty technicznej w zakresie oprogramowania ENOBASE
    - Usługi mogą być wykonywane jedynie przez tych Wykonawców, którzy posiadają niezbędną wiedzę i doświadczenie oraz dysponują odpowiednim potencjałem technicznym i osobami zdolnymi do należytego wykonania zamówienia.
    - Świadczenie usługi asysty technicznej w godzinach od 7.00 do 16.00 od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy.
    - Świadczenie asysty technicznej u Zamawiającego lub zdalnie zgodnie z zasadami zdalnego dostępu.
    - Wykonawca podpisze zasady zdalnego dostępu oraz dołączy listę osób uprawnionych do Zdalnego Dostępu udostępnionego przez Zamawiającego (Imię Nazwisko, adres – e-mail, nr telefonu kontaktowego).
    - Wykonawca podpisze zasady powierzenia przetwarzania danych osobowych.

I. Warunki asysty technicznej

1. Usuwanie błędów w Systemie objętym asystą techniczną wg następujących zasad:
    - Zamawiający określa kategorię błędu, zgodnie z definicją wynikającą z Umowy, w momencie dokonywania zgłoszenia oraz może dokonać jej zmiany na uzasadniony wniosek Wykonawcy.
    - Czas naprawy błędu jest liczony od momentu zgłoszenia do poinformowania Zamawiającego poprzez e-mail o poprawie błędu w Systemie
    - Wykonawca zobowiązuje się do naprawy błędów w sposób zapobiegający utracie jakichkolwiek danych. W przypadku, gdy wykonanie naprawy błędu wiąże się z ryzykiem utraty danych, Wykonawca jest zobowiązany poinformować Zamawiającego o tym przed przystąpieniem do wykonania naprawy błędu.
    - Po poprawie błędu lub wykonaniu obejścia Wykonawca niezwłocznie informuje o tym fakcie Zamawiającego.
    - Po weryfikacji naprawy błędu lub wykonania obejścia Zmawiający niezwłocznie potwierdza skuteczność lub stwierdza nieskuteczność dokonanych czynności Wykonawcy w zakresie poprawy błędu lub dokonania obejścia. Naprawa błędu lub wykonanie obejścia, co do których Wykonawca poinformował o ich wykonaniu, a która/które zostało odrzucone przez Zamawiającego w wyniku przeprowadzonych testów, trwa do czasu jej/jego skutecznego wykonania i potwierdzenia przez Zamawiającego
2. Zamawiający może zgłaszać następujące typy błędów:
    - **Błąd krytyczny**: błąd, w wyniku którego niemożliwe jest użytkowanie systemu w zakresie jego funkcjonalności wskazanej w dokumentacji użytkownika, a w szczególności nieprawidłowe działanie systemu, w wyniku którego następuje zatrzymanie pracy Systemu lub modułu lub niedostępne są istotne funkcje systemu niezbędne do realizacji celów i zadań lub System utracił dane, lub wystąpiły zaburzenia ich integralności, do zastąpienia wadliwej funkcjonalności wymagana jest praca manualna.
    - **Błąd istotny**: działanie Systemu niezgodne z wymaganiami wynikającymi z Umowy oraz z opisanymi w dokumentacji Systemu, w tym dotyczącymi bezpieczeństwa, mające wpływ na poprawne funkcjonowanie Systemu lub jego składowych, odbiegające od standardowego, opisanego w

dokumentacji Systemu, spowodowane błędem oprogramowania lub wadą prac serwisowych/konfiguracyjnych. Błąd istotny to błąd zakłócający rutynową eksploatację Systemu i czynności w pracy bezpośrednich użytkowników - rutynowa eksploatacja Systemu wprawdzie jest możliwa, ale wiąże się z utrudnieniami dla użytkownika (np. spowolnienie reakcji systemu przy otwieraniu okna, zapisywaniu dokumentu, podpisywaniu dokumentu).

- **Błąd zwykły**: błąd nie będący błędem krytycznym ani istotnym i należy przez to rozumieć Stan Systemu, mający wpływ na poprawne funkcjonowanie Systemu lub jego składowych, odbiegający od założeń funkcjonowania Systemu, niezakłócający rutynowej eksploatacji Systemu i czynności w pracy bezpośrednich użytkowników - rutynowa eksploatacja Systemu jest możliwa, ale wiąże się z drobnymi utrudnieniami dla użytkownika (np. wizualizacja dokumentu zawierająca wszystkie wymagane dane ale nieprawidłowo sformatowana; pojawiający się komunikat ostrzegawczy, który nie blokuje funkcjonalności, itp.).
- **Zgłoszenie serwisowe** - w zakresie pomocy przy bieżącej eksploatacji Systemu, zgłoszenie wykonania konkretnej usługi, która nie jest spowodowana błędem w oprogramowaniu, Do zgłoszeń serwisowych Zamawiający zalicza Wszystkie prace wymienione w niniejszym opisie, nie będące błędami i dla których nie określono czasu realizacji.

3. Wykonawca gwarantuje poniższe terminy naprawy błędów:
   - Błąd krytyczny max. 24 godziny robocze
   - Błąd istotny 2 dni roboczych
   - Błąd zwykły 10 dni roboczych
   - Zgłoszenie serwisowe - 10 dni roboczych

   Jeżeli naprawa błędu istotnego nie jest możliwa w czasie naprawy określonym w pkt. 3, dopuszcza się możliwość zastosowania obejścia, przy czym zastosowanie obejścia nie wyłącza zobowiązania Wykonawcy do naprawy błędu, zastosowanie obejścia powoduje zmniejszenie priorytetu błędu do niższej kategorii błędu, z tym, że czas naprawy takiego błędu po zastosowaniu obejścia liczony jest od chwili dokonania zgłoszenia tego błędu;
3. Dostarczanie i wykonywanie aktualizacji Systemu przez Wykonawcę po uzgodnieniu jej zakresu i terminu z Zamawiającym. Aktualizacje mogą zawierać poprawki i rozszerzenia funkcjonalności Systemu zgłoszone także przez innych klientów, a także poprawki i rozszerzenia funkcjonalności wprowadzone przez producenta oprogramowania.
4. Dostosowywanie oprogramowania do wymogów prawa (zgodność, co najmniej w randze rozporządzenia, w rozumieniu art. 87 ust. 1 Konstytucji RP z dnia 2 kwietnia 1997 roku oraz obowiązującymi wykładniami prawnymi lub wskazówkami jednostek nadrzędnych - Narodowy Fundusz Zdrowia, Ministerstwo Zdrowia, Samorządowy Wydział Zdrowia i inne);
5. Przeprowadzenie min. raz w roku strojenia wydajnościowego serwera bazy danych.
6. Zapewnienie działania Systemu w związku ze zmieniającą się technologią np. nowe wersje przeglądarki internetowej, nowe wersje systemów operacyjnych, na których pracuje system).
7. Zarządzanie systemem operacyjnym serwera i serwera kopii bezpieczeństwa Systemu oraz utrzymanie ich w dobrym stanie technicznym z zastrzeżeniem, że Zamawiający zapewni właściwe warunki ich instalacji, a w szczególności: poprawne zasilanie, warunki środowiskowe (np. temperatura, wilgotność, zapylenie), zabezpieczy przed dostępem osób niepowołanych i przed awarią techniczną taką jak przepięcia w sieci zasilającej, zalania itp.
8. Zapewnienie wsparcia technicznego dla sprzętu serwerowego oraz aktualizacji do oprogramowania serwera
9. Administracja Systemem – przed Administrację Systemem Zamawiający rozumie takie czynności jak ponowne instalacje oprogramowania, zmiany konfiguracyjne Systemu na zlecenie Zamawiającego, nadawanie uprawnień zgodnie z zleceniem Zamawiającego, wykonywanie czynności administracyjnych na bazie danych, z której korzysta system, zarządzanie zasobami oraz dbanie o bezpieczeństwo
10. Konsultacje techniczne dotyczące wykorzystania Systemu. Zamawiający ma prawo do konsultacji zdalnych z Wykonawcą bez ograniczeń czasowych w okresie trwania umowy – w odniesieniu do zidentyfikowanych błędów w Systemie. W tym celu Wykonawca udostępni numer telefonu Infolinii. Koszt połączenia z numerem Infolinii będzie naliczany zgodnie z taryfą operatora osoby dzwoniącej.

II. WYMAGANIA DOTYCZĄCE CYERBEZPIECZEŃSTWA

1. Wdrożenie autentykacji wieloskładnikowej (MFA) dla wszystkich kont z dostępem do danych Zamawiającego
2. Instalacja krytycznych aktualizacji naprawiających luki i podatności bezpieczeństwa dla posiadanego oprogramowania – w ciągu 14 dni od oficjalnej publikacji przez producenta oprogramowania
3. Przechowywanie logów dostępu przez minimum 90 dni, Wykonawca zobowiązany będzie do udostępnienia ich na żądanie Zamawiającego w przypadku incydentu
4. Wykonawca jest zobowiązany do szyfrowania danych zarówno "w spoczynku" (dane zapisane na dyskach, w bazach danych lub kopiach zapasowych - AES-256), jak i "w transmisji" (dane przesyłane między użytkownikiem a serwerem np. przez przeglądarkę lub między serwerami - TLS 1.3)

5. Wykonawca ma obowiązek poinformować Zamawiającego o wszelkich incydentach mogących mieć wpływ na bezpieczeństwo dostarczonego oprogramowania wciągu 5 dni od potwierdzenia incydentu. Informacja musi zawierać minimum rodzaj naruszenia, zakres danych, możliwy wpływ na osoby. Wykonawca incydent zgłasza na adres e-mail: …… oraz pod nr telefonu ……
6. Wykonawca jest zobowiązany w przypadku wystąpienia incydentu obejmującego dostarczone oprogramowanie zapewnić wsparcie techniczne w przypadku dochodzenia oraz zapewnić dostęp do systemów na potrzeby analiz.
7. Zamawiający w okresie gwarancji może przeprowadzić coroczne badanie ankietowe Wykonawcy, które będzie miało na celu zweryfikowanie, czy personel Wykonawcy świadczy usługi gwarancyjne zgodnie z procedurami bezpieczeństwa oraz czy systemy lub infrastruktura Wykonawcy chronią prawidłowo powierzone dane.
   Badanie ankietowe będzie zawierało następujące pytania:
   - Czy wyznaczono osoby (osobę) odpowiedzialną za zarządzanie bezpieczeństwem informacji? Jeśli tak, to prosimy o podanie danych kontaktowych.
   - Czy została wdrożona polityka bezpieczeństwa informacji zgodna z ISO 27001 lub równoważna?
   - Czy prowadzony jest formalny rejestr ryzyk i proces jego regularnej aktualizacji?
   - Czy realizowane są cykliczne szkolenia pracowników z bezpieczeństwa?
   - Czy organizacja posiada certyfikaty potwierdzające zgodność (ISO 27001, ISO 22301, SOC 2 lub inne)? Jeśli tak, to prosimy o podanie które.
   - Czy w ostatnich 2 latach przeprowadzono u Wykonawcy audyt bezpieczeństwa (wewnętrzny/zewnętrzny)?
   - Czy został wdrożony proces zapewnienia zgodności z NIS2 (raportowanie incydentów, ochrona danych osobowych)?
   - Czy pracownicy mający dostęp do systemów przechodzą proces weryfikacji (np.. NDA)?
   - Czy stosowane są zasady minimalnych uprawnień i segregacji obowiązków?
   - Czy stosowane są MFA dla wszystkich zdalnych dostępów?
   - Czy wdrożony jest proces monitorowania dostępu do danych i systemów (logowanie, audyt)?
   - Czy wdrożony został formalny plan reagowania na incydenty bezpieczeństwa (IRP)?
   - Czy powołany został zespół reagowania na incydenty?
   - Czy prowadzona jest analiza przyczyn incydentów i raport działań naprawczych?
   - Czy w ciągu ostatnich 3 lat wystąpił incydent poważny/wyciek danych i jakie działania naprawcze wdrożono?
   - Czy wykorzystuje się z podwykonawców w świadczeniu usług dla Zamawiającego?
   - Czy wprowadzony został proces oceny bezpieczeństwa podwykonawców (np. ankiety, audyty)?
   - Czy umowy z podwykonawcami zawierają klauzule bezpieczeństwa (np.. RODO)
   - Czy dostawcy Wykonawcy mają obowiązek raportowania incydentów bezpieczeństwa w określonym czasie?
   - Czy zostały przygotowane plany ciągłości działania (BCP) i odtwarzania po awarii (DRP)?
   - Jakie są gwarantowane czasy odtworzenia (RTO, RPO) dla usług świadczonych dla Zamawiającego?
   - Czy regularnie testowane są scenariusze awaryjne?
   - Czy przygotowana jest redundancja dla kluczowych usług (data center, łącza, zasilanie)?
8. W przypadku wystąpienia zaleceń po przeprowadzeniu badania ankietowego Wykonawca ma obowiązek ich wdrożenia w terminie 30 dni od darty ich otrzymania.

III. ZASADY UDZIELENIA ZDALNEGO DOSTĘPU DO ZASOBÓW

§ 1.
Udostępnienie

1. W celu realizacji usługi asysty technicznej zdalny dostęp zostanie udostępniony Wykonawcy przez Zamawiającego w terminie uzgodnionym przez Strony.
2. Dostęp zdalny ustanawiany jest tylko i wyłącznie do systemów Zamawiającego stanowiących przedmiot umowy.
3. Dostęp zdalny jest możliwy tylko i wyłącznie za pośrednictwem danych autoryzacyjnych udostępnionych Wykonawcy przez Zamawiającego.
4. Zamawiający zobowiązuje się do zapewnienia sprawnego kanału komunikacji.
5. Zamawiający ogranicza zasoby dostępne dla sesji zdalnej do niezbędnego minimum.
6. Zamawiający udostępnia dostęp zdalny z wykorzystaniem systemu PAM, który rejestruje i monitoruje wszystkie zdalne sesje.

§ 2.
Zasady korzystania

1. Korzystając ze Zdalnego Dostępu Wykonawca:

a. będzie wykorzystywał Zdalny Dostęp wyłącznie w celu realizacji przedmiotu umowy;
b. nie będzie pozyskiwał ani przetwarzał żadnych innych danych, za wyjątkiem danych niezbędnych do realizacji przedmiotu umowy;

2. Wykonawca może wnioskować o dane autoryzacyjne tylko i wyłącznie dla osób wykazanych w imiennym wykazie osób upoważnionych do zdalnego dostępu.
3. Zabrania się Wykonawcy przekazywania danych autoryzacyjnych innym osobom niż osoby wskazane w imiennym wykazie osób upoważnionych.
4. Każdy użytkownik zobowiązany jest do stosowania silnych haseł i uwierzytelniania wieloskładnikowego MFA.
5. Liczba użytkowników zdalnego dostępu przyznawanych jednemu Wykonawcy w jednej umowie nie może przekraczać 10 osób, w przypadku systemu PAM w jednym czasie może być aktywnych tylko 5 użytkowników.
6. Po zakończeniu prac w ramach zdalnego dostępu użytkownik zobowiązany się do wylogowania się z wszystkich systemów Zamawiającego i do zakończenia sesji z VPN.
7. Urządzenie wykorzystywane do dostępu zdalnego muszą spełniać minimalne wymogi bezpieczeństwa (aktualny system operacyjny, aktualny antywirus, brak oprogramowania złośliwego).
8. Wykonawca jest zobowiązany do niezwłocznego poinformowania Zamawiającego o zaprzestaniu wykonywania usług będących przedmiotem umowy przez pracownika posiadającego dostęp zdalny.

§ 3.
Warunki Techniczne do uzyskania Zdalnego Dostępu

1. Zamawiający zapewni zdalny dostęp poprzez posiadany przez Zamawiającego system PAM lub w wyjątkowych sytuacjach poprzez bezpieczny kanał VPN;
2. W przypadku dostępu za pośrednictwem systemu PAM, każdy użytkownik otrzyma maila z linkiem do logowania, do systemu PAM, za pośrednictwem którego Zamawiający zapewni pulpit z listą systemów, do których użytkownikowi został udzielony dostęp. Zamawiający nie dopuszcza oprogramowania wykorzystującego obce serwery pośredniczące do komunikacji pomiędzy stronami Umowy
3. Zamawiający przekaże osobie realizującej prace wynikające z zapisów Umowy dane autoryzacyjne
   I. Dla kanału VPN
   a. identyfikator użytkownika (login)
   b. hasło dostępu
   c. parametry niezbędne do zestawienia zdalnego połączenia.
   II. Dla systemu PAM: - link do indywidualnego logowania
4. Użytkownicy po stronie Wykonawcy zobowiązują się do nieudostępniania danych autoryzacyjnych innym osobom oraz wykorzystywania dostępu wyłącznie w celu realizacji niniejszej Umowy.
5. Instalacja oraz konfiguracja przekazanego oprogramowania leżą po stronie pracowników Wykonawcy.

podpis Wykonawcy podpis Zamawiającego

IMIENNY WYKAZ PRACOWNIKÓW WYKONAWCY UPOWAŻNIONYCH DO ZDALNEGO DOSTĘPU

L.p.	Nazwisko i imię	Stanowisko, adres e-mail, nr telefonu
1.		
2.		
3.		
4.		
5.		