Samodzielny Publiczny Zakład Opieki Zdrowotnej
**Szpital Specjalistyczny**
**Ministerstwa Spraw Wewnętrznych i Administracji w Jeleniej Górze**
ul. Cieplicka 69-71 · 58-560 Jelenia Góra
tel. 75 64 35 700 · faks 75 64 35 741
**www.szpitalmsw.net, sekretariat@szpitalmsw.net**

Numer sprawy: 9/2026
Jelenia Góra, 2026-07-02

Strona internetowa
Zamawiającego
www.szpitalmsw.net

**WYJAŚNIENIA TREŚCI SWZ**

dot.: postępowania o udzielenie zamówienia publicznego. Numer sprawy: 9/2026. Nazwa zadania: Świadczenie zarządzanej usługi bezpieczeństwa klasy EDR wraz z usługą SOC/MDR na rzecz SP ZOZ Szpitala Specjalistycznego MSWiA w Jeleniej Górze.

W odpowiedzi na skierowane do zamawiającego zapytania dotyczące treści specyfikacji warunków zamówienia informujemy:

Pytanie — Definicja „innych komponentów usługi”
Wykonawca wnosi o doprecyzowanie katalogu komponentów podlegających licencjonowaniu i/lub monitoringowi, ewentualnie wskazanie zamkniętego wykazu komponentów.
Odpowiedź:
Zamawiający wyjaśnia, że użyte w SWZ i OPZ sformułowanie „inne komponenty usługi” należy rozumieć jako komponenty techniczne niezbędne do prawidłowego uruchomienia, integracji, monitorowania, zarządzania oraz świadczenia usługi EDR/SOC/MDR w zaoferowanym przez Wykonawcę modelu architektonicznym.
Mogą to być w szczególności: agenty, sensory, konektory, parsery, komponenty integracyjne, kolektory, moduły komunikacyjne, komponenty API, komponenty chmurowe, moduły analityczne lub inne równoważne elementy wymagane przez producenta albo Wykonawcę do świadczenia usługi.
Zamawiający nie wprowadza zamkniętego katalogu komponentów, ponieważ architektura rozwiązań EDR/XDR/SOC/MDR może różnić się w zależności od producenta i modelu świadczenia usługi. Jednocześnie Zamawiający podkreśla, że wszystkie komponenty niezbędne do świadczenia zaoferowanej usługi muszą być uwzględnione w cenie oferty i nie mogą powodować dodatkowych kosztów po stronie Zamawiającego, chyba że SWZ wyraźnie stanowi inaczej.
Zmiana treści SWZ:
W Załączniku nr 1 do SWZ — Opis przedmiotu zamówienia — Zamawiający dodaje wyjaśnienie, że przez „inne komponenty usługi” należy rozumieć komponenty techniczne niezbędne do uruchomienia, integracji, monitorowania, zarządzania oraz świadczenia usługi EDR/SOC/MDR, w szczególności agenty, sensory, konektory, parsery, komponenty integracyjne, kolektory, moduły komunikacyjne, komponenty API, komponenty chmurowe, moduły analityczne lub inne

równoważne elementy wymagane przez producenta albo Wykonawcę.

Pytanie — Model wdrożenia EDR, on-premise / cloud / SaaS
Wykonawca wnosi o doprecyzowanie, czy Zamawiający dopuszcza rozwiązania EDR/XDR w architekturze cloud/SaaS.
Odpowiedź:
Zamawiający wyjaśnia, że dopuszcza rozwiązania EDR/XDR/SOC/MDR świadczone w modelu chmurowym, usługowym, hybrydowym, SaaS lub równoważnym, pod warunkiem spełnienia wszystkich wymagań SWZ i OPZ, w szczególności wymagań dotyczących ochrony danych osobowych, bezpieczeństwa informacji, podwykonawców, lokalizacji przetwarzania danych oraz transferów danych poza EOG.
Zamawiający wskazuje, że dokumentacja postępowania nie wymaga dostawy dedykowanego lokalnego serwera zarządzającego EDR po stronie Zamawiającego.
Zmiana treści SWZ:
Zamawiający doprecyzowuje, że użyte w SWZ określenie modelu chmurowego lub usługowego obejmuje również model SaaS, o ile oferowane rozwiązanie spełnia wymagania SWZ i OPZ.

Pytanie — Zakres funkcji rollback
Wykonawca wnosi o doprecyzowanie, czy funkcjonalność rollback dotyczy systemów Windows, czy też innych systemów operacyjnych.
Odpowiedź:
Zamawiający wyjaśnia, że funkcjonalność rollback, remediation, cofnięcia skutków działania złośliwego oprogramowania albo mechanizm równoważny stanowi parametr oceniany w kryteriach pozacenowych, a nie wymaganie minimalne.
Zamawiający dopuszcza, aby zakres tej funkcjonalności był zależny od systemu operacyjnego punktu końcowego oraz możliwości technicznych oferowanego rozwiązania. Wykonawca powinien jednoznacznie wskazać w ofercie lub dokumentacji oferty, dla których systemów operacyjnych i w jakim zakresie oferowana funkcjonalność jest dostępna, w szczególności czy obejmuje środowisko Microsoft Windows.
Ocena punktowa zostanie dokonana na podstawie informacji przedstawionych przez Wykonawcę oraz dokumentów lub opisów potwierdzających spełnienie danego parametru.
Zmiana treści SWZ:
W opisie kryterium dotyczącego funkcji rollback, remediation, cofnięcia skutków działania złośliwego oprogramowania albo mechanizmu równoważnego Zamawiający dodaje zapis:
„Wykonawca zobowiązany jest wskazać w ofercie lub dokumentacji oferty, dla których systemów operacyjnych i w jakim zakresie dostępna jest oferowana funkcjonalność rollback, remediation, cofnięcia skutków działania złośliwego oprogramowania albo mechanizm równoważny. Zamawiający dopuszcza różny zakres tej funkcjonalności w zależności od systemu operacyjnego i możliwości technicznych oferowanego rozwiązania.”

Pytanie — Wymagania wobec dostawcy — ISO/IEC 27001
Wykonawca wnosi o rozważenie wprowadzenia wymogu, aby Wykonawca posiadał certyfikat ISO/IEC 27001 lub równoważny system zarządzania bezpieczeństwem informacji.
Odpowiedź:
Zamawiający przychyla się do wniosku w zakresie potwierdzenia funkcjonowania systemu zarządzania bezpieczeństwem informacji po stronie Wykonawcy lub podmiotu faktycznie świadczącego usługę SOC/MDR.
Zamawiający wyjaśnia, że wymóg ten nie zastępuje pozostałych warunków udziału w postępowaniu określonych w SWZ, w szczególności warunku dotyczącego osób skierowanych do realizacji zamówienia. Wykonawca zobowiązany będzie wykazać spełnienie wszystkich warunków udziału w postępowaniu łącznie.

Zmiana treści SWZ:
W rozdziale VI SWZ — Warunki udziału w postępowaniu — Zamawiający dodaje dodatkowy warunek udziału w postępowaniu w zakresie zdolności technicznej lub zawodowej:
„Niezależnie od warunku dotyczącego osób skierowanych do realizacji zamówienia, o którym mowa w SWZ, Zamawiający wymaga, aby Wykonawca albo podmiot faktycznie świadczący usługę SOC/MDR posiadał ważny certyfikat ISO/IEC 27001 lub certyfikat równoważny, wydany przez niezależną akredytowaną jednostkę certyfikującą, potwierdzający funkcjonowanie systemu zarządzania bezpieczeństwem informacji w zakresie związanym ze świadczeniem usług bezpieczeństwa IT, SOC, MDR, EDR, MSSP, usług zarządzanych IT lub usług równoważnych.
Za certyfikat równoważny Zamawiający uzna certyfikat, który potwierdza funkcjonowanie systemu zarządzania bezpieczeństwem informacji obejmującego co najmniej zarządzanie ryzykiem, kontrolę dostępu, zarządzanie incydentami bezpieczeństwa, ciągłość działania oraz nadzór nad bezpieczeństwem usług świadczonych na rzecz klientów.
Warunek ten podlega spełnieniu łącznie z pozostałymi warunkami udziału w postępowaniu określonymi w SWZ.”
W rozdziale VII SWZ — Wykaz dokumentów składanych wraz z ofertą oraz podmiotowych środków dowodowych — Zamawiający dodaje do podmiotowych środków dowodowych składanych na wezwanie Zamawiającego:
„Certyfikat ISO/IEC 27001 albo dokument równoważny potwierdzający funkcjonowanie systemu zarządzania bezpieczeństwem informacji po stronie Wykonawcy albo podmiotu faktycznie świadczącego usługę SOC/MDR, w zakresie związanym ze świadczeniem usług bezpieczeństwa IT, SOC, MDR, EDR, MSSP lub usług równoważnych.”

Zamawiający informuje, że pytania oraz odpowiedzi na nie stają się integralną częścią specyfikacji warunków zamówienia i będą wiążące przy składaniu ofert.

w związku z udzielonymi wyjaśnieniami zamawiający informuje jednocześnie o utrzymaniu przedłużonego terminu składania ofert. Aktualny termin: 7.07.2026 r. do godz. 10:00 pozostaje bez zmian. Otwarcie ofert nastąpi tego samego dnia o godz.10:30. Pozostałe ustalenia dotyczące miejsca składania i otwarcia ofert pozostają bez zmian.
Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosków o wyjaśnienie treści SWZ.

Signature Not Verified
Dokument podpisany przez Robert Marcin Obaz
Data: 2026.07.02 16:24:43 CEST

Kierownik Zamawiającego

Do wiadomości:
- wszyscy uczestnicy