Wojewódzki Szpital Zespolony w Kielcach
25-736 Kielce, ul. Grunwaldzka 45
tel.: 41/36-71-301, fax: 41/34-50-623
NIP: 959-12-91-292, Regon: 000289785
e-mail: szpital@wszzkielce.pl
www.wszzkielce.pl

ISO 9001

Kielce, dnia 30.05.2023 r.

Znak sprawy: EZ/93/2023/ESŁ

Do wszystkich zainteresowanych

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tekst jednolity: Dz.U. z 2021, poz. 1129 ze zm.) na ***„Świadczenie usług z zakresu cyberbezpieczeństwa dla Wojewódzkiego Szpitala Zespolonego w Kielcach jako Operatora Usługi Kluczowej w celu dostosowania do wymogów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa"***

ODPOWIEDZI NA PYTANIA_2

Zamawiający Wojewódzki Szpital Zespolony w Kielcach działając w oparciu o art. 284 ust. 6 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tekst jednolity: Dz.U. z 2021 r., poz. 1129 ze zm.), przekazuje treść zapytań wraz z wyjaśnieniami:

Pytanie nr 1 do § 1 ust. 2 umowy:
W związku z konieczności oszacowania przez Wykonawcę wartości umowy i ryzykiem jego niedoszacowania, wskazanym § 7 ust. 3 umowy, zwracamy się o usunięcie z treści § 1 ust. 2 pkt. 1) i 3) sformułowań: „w tym", a w pkt. 5) ppkt a) sformułowania „m.in." tak aby zakres prac do wykonania po stronie Wykonawcy stanowił katalog zamknięty, zgodnie z wymaganiami określonymi ustawą o zamówieniach publicznych.
Odpowiedź:
Zamawiający wykreśla:
- w projektowanych postanowieniach umowy w sprawie zamówienia publicznego z treści § 1 ust. 2 pkt 1) i 3) sformułowanie „w tym" i z pkt 5) ppkt a) sformułowanie „m.in."
- w szczegółowym opisie przedmiotu zamówienia (SOPZ) z treści pkt 1 i 3 sformułowanie: „w tym" i z treści pkt 5 sformułowanie „m.in."
- w SWZ z treści pkt 3 ppkt a i c) sformułowanie: „w tym" i z treści pkt 3 ppkt e) tiret 1 sformułowanie „m.in.".

Pytanie nr 2 do § 3 ust. 8 umowy:
Zwracamy się o ograniczenie odpowiedzialności Wykonawcy określonej umową wyłącznie do zdarzeń powstałych z winy Wykonawcy, zgodnie z zapisami Kodeksu Cywilnego oraz zgodnie z dyspozycją art. 433 pkt. 1) ustawy z dnia 11.09.2019 r. Prawo zamówień publicznych – odpowiedzialność na zasadzie winy i zmianę treści § 3 ust. 8 umowy w sposób następujący: „8. Wykonawca ponosi odpowiedzialność za wszelkie **zawinione** szkody wyrządzone Zamawiającemu lub osobom trzecim w związku z realizacją niniejszej Umowy."
Odpowiedź:
Zamawiający w projektowanych postanowieniach umowy w sprawie zamówienia publicznego zmienia treść § 3 ust. 8 umowy w sposób następujący: „8. Wykonawca ponosi odpowiedzialność za wszelkie szkody wyrządzone Zamawiającemu lub osobom trzecim w związku z realizacją niniejszej Umowy, chyba że wyłączna odpowiedzialność za powstanie danych okoliczności jest spowodowana działaniem lub zaniechaniem ze strony Zamawiającego."

Pytanie nr 3 do § 3 umowy:
Zwracamy się o dodanie w treści § 3 kolejnego ustępu 10 o treści: „10. Całkowita odpowiedzialność Wykonawcy z tytułu umowy ograniczona jest do wartości umowy określonej § 7 ust. 9 z wyłączeniem utraconych korzyści oraz z uwzględnieniem powszechnie obowiązujących przepisów prawa."
Odpowiedź:
Zamawiający odmawia wprowadzenia proponowanego postanowienia do projektowanych postanowieniach umowy w sprawie zamówienia publicznego.

Pytanie nr 4 do § 5 ust. 1 lit a) umowy:
Zwracamy się o doprecyzowanie § 5 ust. 1 lit a) umowy jak niżej:
„a) współpracę w zakresie planowania oraz realizowania przez Wykonawcę czynności w ramach przedmiotu Umowy,".
Odpowiedź:
Zamawiający w projektowanych postanowieniach umowy w sprawie zamówienia publicznego poprawia treść § 5 ust. 1 lit a) w sposób następujący: „a) współpracę w zakresie planowania oraz realizowania przez Wykonawcę czynności w ramach przedmiotu Umowy,"

Pytanie nr 5 do § 5 ust. 2 pkt. a) i b) umowy.
Prosimy o potwierdzenie czy Zamawiający dopuszcza, aby spotkania i narady o jakich mowa. w § 5 ust. 2 pkt. a) i b) umowy odbywały się w trybie zdalnym.
Odpowiedź:
Zamawiający nie precyzował w opisie przedmiotu zamówienia oraz umowie trybu spotkań i narad jednocześnie informuje, iż spotkania i narady mogą się odbywać w trybie zdalnym.

Pytanie nr 6 do § 9 ust. 2 lit. f) umowy.
Zwracamy się o doprecyzowanie § 9 ust. 2 lit. f) umowy jak niżej:
„f) w przypadku nałożenia przez uprawnione zewnętrzne organy kontrolne kary pieniężnej na Zamawiającego wskutek nienależytego świadczenia przez Wykonawcę usług **wskazanych § 7 ust. 1 pkt. b) umowy**, w szczególności w przypadkach określonych w art. 73 ustawy z dnia z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, oprócz obowiązku zapłaty przez Wykonawcę kwoty kary, Wykonawca zobowiązany będzie do zapłaty na rzecz Zamawiającego kary umownej w wysokości 2% kwartalnego wynagrodzenia brutto Wykonawcy, o którym mowa w § 7 ust 1 pkt b)."
Odpowiedź:
Zamawiający odmawia wprowadzenia proponowanego postanowienia do projektowanych postanowieniach umowy w sprawie zamówienia publicznego.

Pytanie nr 7 do § 9 ust. 4 umowy.
Zwracamy się o doprecyzowanie § 9 ust. 4 umowy jak niżej:
„4. Zamawiający zastrzega sobie prawo potrącenia kar umownych oraz **kar pieniężnych**, o których mowa w umowie, z wynagrodzenia należnego Wykonawcy. O potrąceniu Zamawiający zawiadomi Wykonawcę w formie pisemnej wraz z podaniem uzasadnienia."
Odpowiedź:
Zamawiający odmawia wprowadzenia proponowanego postanowienia do projektowanych postanowieniach umowy w sprawie zamówienia publicznego.

Pytanie nr 8 do § 11 ust. 5 umowy:
Zwracamy się o ograniczenie odpowiedzialności Wykonawcy wyłącznie do roszczeń zasądzonych prawomocnym orzeczeniem sądu, a nie do każdego, nawet najbardziej bezzasadnie zgłoszonego roszczenia

przez osobę trzecią, jak wynika z obecnej treści umowy i zmianę treści § 11 ust. 5 umowy jak niżej: „5. Zamawiający nie ponosi odpowiedzialności za naruszenie autorskich praw majątkowych lub osobistych wobec osób trzecich. Wykonawca zobowiązuje się do nieodwołalnego i bezwarunkowego zwolnienia Zamawiającego, na pierwsze żądanie, z wszelkich roszczeń, wynikających z naruszenia majątkowych i osobistych praw autorskich, do którego doszło z przyczyn leżących po stronie Wykonawcy, **zasądzonych prawomocnym orzeczeniem sądu**.".

Odpowiedź:
Zamawiający odmawia wprowadzenia proponowanego postanowienia do projektowanych postanowieniach umowy w sprawie zamówienia publicznego.

Pytanie nr 9 do § 13 ust. 3) pkt. e) umowy:
Zwracamy się o doprecyzowanie treści umowy i w miejsce wskazanych w § 13 ust. 3 pkt. e) „tożsamych obowiązków określonych w umowie" wprowadzenie skonkretyzowanych obowiązków określonych umową, poprzez odwołanie do właściwej części umowy.

Odpowiedź:
W ocenie Zamawiający postanowienie w § 13 ust. 3 pkt. e) nie wymaga dodatkowej regulacji. Strony mają w umowie czytelnie określone prawa i obowiązki.

Pytanie nr 10 do § 13 ust. 6) umowy:
Zwracamy się o wydłużenie terminu w § 13 ust. 6 umowy do 14 dni.

Odpowiedź:
Zamawiający nie wyraża zgody na wydłużenie terminu w § 13 ust. 6 umowy do 14 dni.

Pytanie nr 11 Dot. Warunki udziału w postępowaniu punkt 1 pp. a)
Zamawiający wymaga „w okresie ostatnich **trzech lat** przed upływem terminu składania ofert (a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie) lub aktualnie realizują **co najmniej dwie usługi, których przedmiotem było świadczenie usługi Security Operation Center (SOC) przez okres minimum 12 miesięcy** na rzecz Zamawiającego, którym jest jednostka służby zdrowia **wyznaczoną do pełnienia funkcji Operatora Usług Kluczowej** w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U. z 2022 r. poz.1863)". Poziom i jakość świadczonej usługi SOC jest na takim samym poziomie niezależnie od gałęzi gospodarki czy statusu prawnego podmiotu objętego ochroną. Czy Zamawiający wyrazi zgodę na modyfikację powyższego wymagania w następujący sposób: „w okresie ostatnich **trzech lat** przed upływem terminu składania ofert (a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie) lub aktualnie realizują **co najmniej dwie usługi, których przedmiotem było świadczenie usługi Security Operation Center (SOC) przez okres minimum 12 miesięcy** na rzecz Zamawiającego.

Odpowiedź:
Zamawiający modyfikuje SWZ w punkcie 11 ppkt 1) lit. a) SWZ który otrzymuje brzmienie:
„zrealizowali należycie w okresie ostatnich trzech lat przed upływem terminu składania ofert (a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie) lub aktualnie realizują co najmniej dwie usługi, których przedmiotem było świadczenie usługi Security Operation Center (SOC) przez okres minimum 12 miesięcy, w tym jednej na rzecz Zamawiającego, którym jest jednostka służby zdrowia wyznaczoną do pełnienia funkcji Operatora Usługi Kluczowej w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U. z 2022 r. poz.1863)",

Pytanie nr 12 Dot. Warunki udziału w postępowaniu punkt 1 pp. b)
Zamawiający wymaga „zrealizowali należycie w okresie ostatnich **trzech lat** przed upływem terminu składania ofert (a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie) **co najmniej dwie**

kompleksowe usługi, których przedmiotem było dostosowanie Zamawiającego do spełnienia wymogów określonych dla Operatora Usług Kluczowych (OUK) w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U. z 2022 r. poz.1863) **o wartości umowy brutto min 50.000,00 zł** w tym **jedna z usług winna obejmować wykonanie analizy śledczej (forensic)** *rozumianej wg SOPZ pkt 7*. Pragniemy zauważyć, że usługa analizy śledczej (forensic), rozumianej wg SOPZ pkt 7, jest odrębną usługą nie powiązaną z usługą dostosowania Zamawiającego do spełnienia wymogów określonych dla Operatora Usług Kluczowych (OUK). W związku z tym czy Zamawiający wyrazi zgodę na przedstawienie dwóch niezależnych realizacji, jednej na dostosowanie Zamawiającego do spełnienia wymogów określonych dla Operatora Usług Kluczowych (OUK), i drugiej na wykonanie analizy śledczej (forensic) rozumianej wg SOPZ pkt 7.

Odpowiedź:

Tak, Zamawiający dopuszcza przedstawienie dwóch niezależnych realizacji, jednej na dostosowanie Zamawiającego do spełnienia wymogów określonych dla Operatora Usług Kluczowych (OUK), i drugiej na wykonanie analizy śledczej (forensic) rozumianej wg SOPZ pkt 7.

Pytanie nr 13 Dot. Warunki udziału w postępowaniu punkt 1 pp. c)

Zamawiający wymaga: „zrealizowali należycie w okresie ostatnich **trzech lat** przed upływem terminu składania ofert (a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie) **co najmniej dwie usługi których przedmiotem było wykonanie audytu bezpieczeństwa** w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U. z 2022 r. poz.1863) **systemu informacyjnego, dla jednostki wyznaczonej do pełnienia funkcji Operatora Usług Kluczowej,**" Poziom i jakość świadczonej usługi wykonania audytu bezpieczeństwa jest niezależna od gałęzi gospodarki czy statusu prawnego podmiotu objętego ochroną. Czy Zamawiający wyrazi zgodę na modyfikację powyższego wymagania w następujący sposób: „zrealizowali należycie w okresie ostatnich **trzech lat** przed upływem terminu składania ofert (a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie) **co najmniej dwie usługi których przedmiotem było wykonanie audytu bezpieczeństwa** w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U. z 2022 r. poz.1863) **systemu informacyjnego"**

Odpowiedź:

Zamawiający wyjaśnia, iż nie ograniczał spełnienie tego warunku do jednostek służby zdrowia, a jedynie wskazywał, że spełnieniem warunku będzie wykonanie audytu bezpieczeństwa w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U. z 2022 r. poz.1863) systemu informacyjnego, dla jednostki wyznaczonej do pełnienia funkcji Operatora Usług Kluczowej, bez względu na gałąź gospodarki czy status prawny jednostki audytowanej.

Pytanie nr 14 Dot. Warunki udziału w postępowaniu punkt 1 pp. d)

Warunek: "**co najmniej trzech** ekspertów posiada doświadczenie zdobyte w okresie ostatnich **pięciu lat** przed upływem terminu składania ofert polegające na pracy **przez okres min. 24 miesięcy w projektach obejmujących świadczenie usługi Security Operation Center w ramach świadczenia usługi Operatora Usług Kluczowych,**" Poziom i jakość świadczonej usługi SOC jest niezależna od gałęzi gospodarki czy statusu prawnego podmiotu objętego ochroną. Czy Zamawiający wyrazi zgodę na modyfikację powyższego wymagania do formy "co najmniej trzech ekspertów posiada doświadczenie zdobyte w okresie ostatnich pięciu lat przed upływem terminu składania ofert polegające na pracy przez okres min. 24 miesięcy w projektach obejmujących świadczenie usługi Security Operation Center".

Odpowiedź:

Zamawiający modyfikuje SWZ w punkcie 11 ppkt 1d) tiret 1, który otrzymuje brzmienie:
„co najmniej trzech ekspertów posiada doświadczenie zdobyte w okresie ostatnich pięciu lat przed upływem terminu składania ofert polegające na pracy przez okres **min. 12 miesięcy** w projektach obejmujących świadczenie usługi Security Operation Center w ramach świadczenia usługi Operatora Usług Kluczowych,"

Pytanie nr 15 Dot. Katalog certyfikatów
Czy Zamawiający uzna za spełniony wymóg posiadania certyfikatu RHCSA (Red Hat Certified System Administrator Red Hat Enterprise Linux 6) w przypadku gdy Wykonawca wykaże się dysponowaniem osobą legitymującą się nowszym certyfikatem RHCSA (Red Hat Certified System Administrator Red Hat Enterprise Linux 7) ?
Odpowiedź:
Tak zamawiający uzna za spełniony wymóg posiadania certyfikatu RHCSA (Red Hat Certified System Administrator Red Hat Enterprise Linux 7), jako nowszy i równoważny opisanemu w SWZ jako RHCSA (Red Hat Certified System Administrator Red Hat Enterprise Linux 6).

Pytanie nr 16 Dot. OPZ - Szacowanie ryzyka
Czy zamawiający posiada inwentaryzacje aktyw i zmapowanie procesów wspierających działanie usługi kluczowej, jeżeli nie to czy zleceniobiorca ma dokonać inwentaryzacji aktyw oraz mapowania procesów wspierających usługę kluczową?
Odpowiedź:
Zamawiający informuje, iż nie posiada inwentaryzacji aktyw i zmapowanych procesów wspierających działanie usługi kluczowej, i Wykonawca ma dokonać inwentaryzacji aktyw oraz mapowania procesów wspierających usługę kluczową w ramach realizacji przedmiotu umowy.

Pytanie nr 17 Dot. OPZ - Szacowanie ryzyka
W decyzji właściwego ministra został wyodrębniony zakres usługi kluczowej. Proszę o informacje jakie usługi kluczowe zostały w szpitalu objęte decyzją Ministra?
Odpowiedź:
Zamawiający przedstawił usługi kluczowe objęte decyzją o wyznaczeniu Szpitala na Operatora Usługi Kluczowej w preambule wzoru umowy, którą przytacza poniżej:
„Podstawą realizacji umowy jest decyzja z dnia 07 lipca 2022 r. o uznaniu Wojewódzkiego Szpitala Zespolonego w Kielcach za operatora usługi kluczowej w sektorze ochrony zdrowia, polegającej na:
1) udzielaniu świadczeń opieki zdrowotnej przez podmiot leczniczy,
2) obrocie i dystrybucji produktów leczniczych."

Pytanie nr 18 Dot. OPZ - Szacowanie ryzyka pp b)
Proszę określić co ile ma być przeprowadzany okres szacowania ryzyka, gdyż on powinien być systematyczny (raz na dany okres) oraz po planowaniu i wdrażaniu istotnych zmian w świadczonym procesie?
Odpowiedź:
Szacowanie ryzyka, powinno odbywać się zgodnie z wymaganiami określonymi w Ustawie o KSC oraz w rozporządzeniach wykonawczych, obowiązujących w tym zakresie.

Pytanie nr 19 Dot. OPZ - Szacowanie ryzyka
Czy analiza ryzyka w zakresie bezpieczeństwa informacji ma uwzględniać wymagania normy ISO 27005?
Odpowiedź:
Zamawiający nie precyzuje szczególnych wymagań w tym zakresie poza tymi opisanymi w OPZ i wynikającymi z obowiązujących przepisów w tym zakresie.

Pytanie nr 20 Dot. OPZ - Wymagania dla usługi Security Operations Center (SOC) pp. 2.1.1
Czy w myśl tego zapisu zamawiający oczekuje audytu bezpieczeństwa zgodnie z wymaganiami UKSC dot. przeprowadzania audytu?
Odpowiedź:

Wojewódzki Szpital Zespolony w Kielcach
25-736 Kielce, ul. Grunwaldzka 45
tel.: 41/36-71-301, fax: 41/34-50-623
NIP: 959-12-91-292, Regon: 000289785
e-mail: szpital@wszzkielce.pl
www.wszzkielce.pl

Zamawiający wyjaśnia, iż w opisie OPZ pkt. 2.1.1. oczekuje audytu infrastruktury Zamawiającego w celu zidentyfikowania kluczowych zasobów teleinformatycznych do świadczenia usług kluczowych, które powinny być objęte usługą SOC.

Pytanie nr 21 Dot. OPZ - Wymagania dla usługi Security Operations Center (SOC) pp. 2.1.2 b)
Proszę o informację czy jest do tego SLA są także liczone przerwy w działaniu SOC niezbędne do przeprowadzania prac serwisowych np. aktualizacji oprogramowania oraz serwerów na których stoi usługa?
Odpowiedź:
Tak, do SLA są także liczone przerwy w działaniu SOC niezbędne do przeprowadzania prac serwisowych np. aktualizacji oprogramowania oraz serwerów, z wyjątkiem przerw technicznych uzasadnionych względami bezpieczeństwa, zaplanowanych z Zamawiającym i w terminie uzgodnionym z Zamawiającym.

Pytanie nr 22 Dot. OPZ - Wymagania dla usługi Security Operations Center (SOC) pp. 2.1.3
Jakimi środkami redundantnymi dysponuje szpital w przypadku braku dostępu do systemu (SIEM, Kolektor) w przypadku awarii łącza po stronie zamawiającego oraz w przypadkach awarii serwerów?
Odpowiedź:
Szpital posiada łącze podstawowe i zapasowe zapewniające dostęp do sieci Internet, instalacja oprogramowania kluczowych systemów odbywa się z zachowaniem zasady odporności systemu na awarię pojedynczego elementu.

Pytanie nr 23 Dot. OPZ - Wymagania dla usługi Security Operations Center (SOC) pp. 2.1.4 f)
Proszę o informacje w jakim zakresie ma być udzielane wsparcie w zakresie bezpieczeństwa?
Odpowiedź:
Zamawiający informuje, iż oczekuje wsparcia Wykonawcy w zakresie konsultacji i doradztwa w zakresie projektowania i doboru systemów bezpieczeństwa adekwatnych do posiadanego środowiska teleinformatycznego i zidentyfikowanych ryzyk.

Pytanie nr 24 Dot. OPZ - Wymagania dla usługi Security Operations Center (SOC) pp. 2.1.4 g)
W jaki sposób ma to być realizowane? Proszę o podanie szacowanych godzin w miesiącu niezbędnych na konsultacje w ramach trwania umowy.
Odpowiedź:
Zamawiający informuje, iż oczekuje wsparcia Wykonawcy w zakresie konsultacji i doradztwa w zakresie zarządzania zgodnością działalności z normami, zaleceniami i stosowanymi praktykami, stosownie do zidentyfikowanych potrzeb w tym zakresie. Zamawiający nie określa limitu godzin/ nie przewiduje więcej niż 2 godziny /m-c.

Pytanie nr 25 Dot. OPZ - Wymagania dla usługi Security Operations Center (SOC) pp. 2.2 c)
W jakiej formie mają być konsultacje?
Odpowiedź:
Zamawiający oczekuje konsultacji w formie doradztwa merytorycznego i technicznego.

Pytanie nr 26 Dot. OPZ - Wymagania dla usługi Security Operations Center (SOC) pp. 2.3 f)
Czy w myśl zapisu zamawiający rozumie np. przeprowadzenie prac aktualizacyjnych w jego infrastrukturze, szkolenie pracowników, dodanie odpowiedniego IoC do systemów bezpieczeństwa przez wykonawcę czy rozumie ten punkt jako wsparcie przy przygotowaniu rekomendacji, gdzie organizacja wdraża je samodzielnie?
Odpowiedź:

Zamawiający oczekując wsparcia przy wdrożeniu rekomendacji po wystąpieniu incydentu, oczekuje przygotowania rekomendacji, oraz pomoc i konsultacji technicznych przy ich wdrożeniu przez Zamawiającego.

Pytanie nr 27 Dot. OPZ - Wymagania dla usługi Security Operations Center (SOC) pp. 2.5 f)
Proszę o dokładny opis jakie są to punkty np. logi z firewalla, logi z WAF, logi z EDR/XDR, itp…
Odpowiedź:
Określenie punktów monitorowania, objętych usługą SOC, jest przedmiotem usługi i wynika z punktu 2.1.1.

Pytanie nr 28 Dot. OPZ - Wymagania dla usługi Security Operations Center (SOC) pp. 2.5 g)
Proszę o określenie progu o ile może wzrosnąć wymagana liczba monitorowanych punktów?
Odpowiedź:
Określenie punktów monitorowania, objętych usługą SOC, jest przedmiotem usługi i wynika z punktu 2.1.1., Zamawiający nie przewiduje znaczącego wzrostu liczby monitorowanych punktów (ponad 100 zakładanych), jednocześnie docelowa liczba będzie uzależniona od wyników szacowania ryzyka i bieżącej analizy zdarzeń.

Pytanie nr 29 Dot. OPZ - Wymagania dla usługi Security Operations Center (SOC) pp. 2.7)
Proszę o informacje w jakim zakresie ma być udzielane wsparcie w zakresie bezpieczeństwa? Jaki jest szacunkowy czas rbh?
Odpowiedź:
Zamawiający informuje, iż w tym zakresie oczekuje od Wykonawcy usługi, świadczonej w formie konsultacji, doradztwa i nadzoru eksperckiego w zakresie opisanym w OPZ. Zamawiający nie określa limitu godzin/ nie przewiduje więcej niż 2 godziny /m-c.

Pytanie nr 30 Dot. OPZ – 4.
Opracowanie dokumentacji dla Szpitala dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej zgodnie z Rozporządzeniem Rady Ministrów z dnia 16 października 2018 r w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz.U. z 2018 r. poz. 2080). Czy zamawiający ogólnie posiada następujące polityki: Polityka Bezpieczeństwa Informacji, Polityka Zarządzania Zasobami Informatycznymi, Polityka Ciągłości Działania, Procedura Analizy Ryzyka, Polityka Bezpieczeństwa Fizycznego, Plan Ciągłości Działania (BCP + DRP) lub inne tego typu polityki i procedury (jeżeli tak to jakie)?
Odpowiedź:
Zamawiający w tym zakresie posiada Politykę Bezpieczeństwa Przetwarzania Danych Osobowych oraz Instrukcję Zarządzania Systemami Informatycznym.

Pytanie nr 31 Dot. OPZ – 7.
Wspieranie Zamawiającego w zakresie: identyfikowania zagrożeń w odniesieniu do systemów informacyjnych; analizowania oprogramowania szkodliwego i określania jego wpływu na system informacyjny Zamawiającego; zabezpieczania śladów kryminalistycznych na potrzeby postępowań prowadzonych przez organy ścigania. pp 7.b - okoliczności wytworzenia oprogramowania,
W jaki sposób ma być ten zakres realizowany? UKSC nie wspomina o realizacji tego zadania. Wnioskujemy o wykreślenie tego zapisu, gdyż jest on niejasny oraz okoliczności napisania złośliwego kodu w wielu przypadkach są nieznane.
Odpowiedź:
Ten zakres usługi, wynika z Rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019r., w szczególności par.1, pkt 4). Zamawiający nie określa szczegółowych wymagań jakimi metodami Wykonawca będzie

realizował tą usługę, poza tymi już określonymi w OPZ i opisanymi w przytoczonym Rozporządzeniu Ministra Cyfryzacji.

Pytanie nr 32
W związku z krótkim okresem czasu, który pozostanie wykonawcom na zapoznanie się z odpowiedziami Zamawiającego na pytania oraz dużą ilością dokumentów, które należy załączyć do oferty zwracamy się z prośbą przedłużenie terminu składania ofert na dzień 07.06.2023r.
Odpowiedź:
Zamawiający, w celu wypełnienia dyspozycji art. 284 ust. 2 w powiązaniu z art. 286 ust. 3 ustawy PZP, przedłuża termin składania i otwarcia ofert w przedmiotowym postępowaniu.
Nowy termin składania i otwarcia ofert wyznacza się na:

- termin składania ofert: **05.06.2023 r. - godz. 9:00**
- termin otwarcia ofert: **05.06.2023 r. - godz. 9:30**

W związku ze zmianą terminu składania i otwarcia ofert Zamawiający zmienia treść **pkt 23 SWZ *Termin związania ofertą***, nadając mu nowe brzmienie: *„Termin związania ofertą wynosi 30 dni, tj. Wykonawca jest związany ofertą **do dnia 04.07.2023 r.** Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert".*

Pytanie nr 33
Pytanie dot. punktu 11 ppkt 1) lit. a):
Z uwagi na specyficzny sposób kontraktowania usług typu SOC w branży ochrony zdrowia (vide finansowanie z Zarządzenia 68 w roku 2022), gdzie niezmiernie rzadko zdarzają się długofalowe kontrakty na świadczenie usługi SOC czy choćby na taką usługę przez okres 12 miesięcy (a nie do końca bieżącego roku jak ma to miejsce zazwyczaj) - czy Zamawiający uzna za wystarczający dowód zdolności technicznych i doświadczenia zawodowego wykonawcy świadczącego usługi SOC dla podmiotów branży ochrony zdrowia wyznaczonych na Operatorów Usług Kluczowych, w sytuacji gdy wykonawca przedstawi dowód świadczenia usługi SOC przez nie mniej niż 12 miesięcy dla dwóch podmiotów, z których jednym jest jednostka służby zdrowia wyznaczona na Operatora Usługi Kluczowej?
Odpowiedź:
Brzmienie warunku udziału w postepowaniu zgodnie z odpowiedzią na pytanie nr 11 dot. warunki udziału w postępowaniu.

Pytanie nr 34
W związku z 1pkt. Załącznika nr.2 do SWZ, ile zamawiający posiada usług kluczowych w otrzymanej decyzji?
Odpowiedź:
Zamawiający przedstawił usługi kluczowe objęte decyzją o wyznaczeniu Szpitala na Operatora Usługi Kluczowej w preambule wzoru umowy, którą przytacza poniżej:
„Podstawą realizacji umowy jest decyzja z dnia 07 lipca 2022 r. o uznaniu Wojewódzkiego Szpitala Zespolonego w Kielcach za operatora usługi kluczowej w sektorze ochrony zdrowia, polegającej na:
1) udzielaniu świadczeń opieki zdrowotnej przez podmiot leczniczy,
2) obrocie i dystrybucji produktów leczniczych."

Pytanie nr 35
W związku z 1pkt, załącznika nr.2 do SWZ jak dużą infrastrukturę posiada Zamawiający zidentyfikowana jako pracująca na rzecz usług kluczowych, w rozróżnieniu na:
-Serwery (szt.)
-Systemy informatyczne (jakie)
-Urządzenia sieciowe (jakie, szt.)

-Systemy backupu (jakie, szt.)
-Serwerownie, pomieszczenia dystrybucyjne
-Ilość lokalizacji (ilość oraz skala)

Odpowiedź:
Zamawiający informuje, iż nie posiada inwentaryzacji aktywów i zmapowanych procesów wspierających działanie usługi kluczowej, i Wykonawca ma dokonać inwentaryzacji aktywów oraz mapowania procesów wspierających usługę kluczową w ramach realizacji przedmiotu umowy, zgodnie z Załącznikiem nr 2 do SWZ Pkt 1 ppkt a) oraz Pkt 2. Ppkt 2.1.1. Dla zobrazowania wielkości infrastruktury Zamawiający informuje, iż posiada 4 główne lokalizacje w obrębie jednego Miasta, wielopawilonową zabudowę, około 1000 stacji roboczych, 3 pomieszczenia pełniące funkcje serwerowni, przybliżona liczba użytkowników systemów wynosi 2000.

Pytanie nr 36
W związku z punktem 2, załącznika nr.2 do SWZ, jak dużą infrastrukturę Zamawiający zamierza przeznaczyć do monitorowania?

Odpowiedź:
Określenie punktów monitorowania, objętych usługą SOC, jest przedmiotem usługi i wynika z Załącznika nr 2 do SWZ Pkt 2.1.1. oraz 2.5 f)-g).

Pytanie nr 37
W związku z punktem 2, załącznika nr.2 do SWZ, jaka jest szacunkowa wielkość dzienna plików logów infrastruktury Zamawiającego obejmująca zdarzenia z urządzeń takich jak:(w GB)?
-Węzeł bezpieczeństwa
-Serwery
-Urządzenia sieciowe
-Backup
-Endpointy
-Inne..

Odpowiedź:
Zamawiający nie posiada szczegółowej analizy w tym zakresie, zgodnie z **Załącznikiem nr 2 do SWZ Pkt 2. ppkt 2.1.1** *„Wdrożenie i świadczenie usługi SOC poprzedzone jest audytem teleinformatycznym infrastruktury klienta, dzięki czemu możliwe jest dokonanie inwentaryzacji, wskazanych kluczowych serwerów oraz optymalizacja prac wdrożeniowych SOC."*

Pytanie nr 38
W związku z punktem 3. załącznika nr.2 do SWZ, na jakim poziomie Zamawiający przewiduje przygotować dokumentacje?
-Polityki
-Polityki, procedury
-Polityki, procedury, instrukcje
Od oczekiwanego poziomu uzależnione jest również Państwa dostępność i zaangażowanie.

Odpowiedź:
Zamawiający informuje iż w Załączniku nr 2 do SWZ a szczególnie w Pkt 4. zawarł wymagania dotyczące opracowania dokumentacji dla Szpitala dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Zamawiający deklaruje zaangażowanie i współpracę z Wykonawcą w realizacji przedmiotu umowy.

Wojewódzki Szpital Zespolony w Kielcach
25-736 Kielce, ul. Grunwaldzka 45
tel.: 41/36-71-301, fax: 41/34-50-623
NIP: 959-12-91-292, Regon: 000289785
e-mail: szpital@wszzkielce.pl
www.wszzkielce.pl

Pytanie nr 39
W związku z 6pkt. Załącznika nr. 2 do SWZ, ile godzin Zamawiający planuje wykorzystać w zakresie doboru i wdrażania środków technicznych i organizacyjnych mających wpływ na bezpieczeństwo teleinformatyczne Szpitala?
Odpowiedź:
Zamawiający nie określa limitu godzin w tym zakresie, zaangażowanie Wykonawcy w zapewnieniu wsparcia Zamawiającego i konsultacji w zakresie doboru i wdrażania środków technicznych i organizacyjnych będzie wynikało z szacowania ryzyka, które jest w zakresie usług objętych Umową.

Pytanie nr 40
W związku z pkt. 7. załącznika nr. 2 do SWZ, czy Zamawiający ma na myśli standardowe audyty podatności, jeżeli tak to jaką ich ilość w roku przewiduje?
Odpowiedź:
Zamawiający, nie precyzuje dokładnych metod jakimi Wykonawca będzie realizował zakres usług opisanych w Załączniku nr 2 do SWZ Pkt 7. Zakłada, że Wykonawca będzie przeprowadzał również standardowe audyty podatności w ilości niezbędnej do spełnienia wymogów określonych w Rozporządzeniu ministra Cyfryzacji z dnia 4 grudnia 2019r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.

Odpowiedzi na pytania zawarte w niniejszym piśmie oraz wprowadzone modyfikacje są wiążące i należy uwzględnić je w treści składanej oferty.

Z-CA DYREKTORA
ds. lecznictwa
Krzysztof Bidas

KIEROWNIK
Działu Zamówień Publicznych
mgr Sebastian Skaniawski

DZIAŁ ZAMÓWIEŃ PUBLICZNYCH
mgr Edyta Słowińska
SPECJALISTA