Znak sprawy: DZP.271.36.2023

załącznik nr 5 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. ZAKRES ROBÓT

1.1 KOD I NAZWA KODU CPV:

Kod CPV:

48180000 – Pakiety oprogramowania medycznego

30210000- Maszyny do przetwarzania danych (sprzęt)

1.2 ZAKRES RZECZOWY PRZEDMIOTU ZAMÓWIENIA

W związku z wdrożeniem platformy regionalnej eCareMed w Beskidzkim Centrum Onkologii - Szpital Miejski im. Jana Pawła II przy ulicy Wyzwolenia 18, powstała konieczność rozbudowy infrastruktury sprzętowej i informatycznej w celu spełnienia wymogów zawartych w dokumentacji technicznej dla wyżej wymienionego projektu. Zamawiający ogłasza nabór ofert na dostawę urządzeń oraz oprogramowania służącego do realizacji przedmiotowego zadania.

Zadanie dotyczy zakupu, dostawy i montażu kompletnego zestawu urządzeń wraz z , oprogramowaniem (licencja) zgodnych z poniższymi wymaganiami:

1) Dostawa, montaż i uruchomienie dwóch kompletów serwerów według niżej podanej specyfikacji ,
2) Dostawa i uruchomienie systemu Web Aplication Firewall (dalej WAF)

Zamawiający wymaga również, przed przystąpieniem do powyżej opisanych prac dostarczenia projektu wykonawczego zawierającego co najmniej:.

1) Opis sposobu podłączenia i integracji dostarczonych urządzeń z infrastrukturą Zmawiającego.
2) Projekt konfiguracji sytemu WAF.

Przed planowanym montażem Wykonawca dokona weryfikacji istniejących instalacji teletechnicznych i dokonać szerokiej konsultacji z Zamawiającym. Przeprowadzone konsultacje powinny dotyczyć uzgodnień technicznych w zakresie ostatecznej lokalizacji urządzeń, integracji z infrastrukturą, konfiguracji sprzętowej i oprogramowania oraz wszelkich innych elementów dostarczanego związanych z prawidłowym wykonaniem projektu.

Zamawiający udostępni wszelkie pozostające w jego dyspozycji dokumenty i informacje dotyczące infrastruktury teleinformatycznej oraz funkcjonującego oprogramowania..

Koordynacja prac montażowych powinna być dokonana we wszystkich fazach procesu, w szczególności należy przedstawić szczegółowy harmonogram związany z realizacją projektu.

Wszystkie stosowane materiały i urządzenia muszą być fabrycznie nowe i dobrej jakości, a także muszą dokładnie odpowiadać warunkom niezbędnym do prawidłowego wykonania powierzonych prac oraz do

poprawnego funkcjonowania całej konfiguracji. Stosowane materiały i urządzenia muszą posiadać wymagane deklaracje zgodności lub certyfikaty dopuszczające do stosowania na terenie Unii Europejskiej.

Wszelkie uszkodzenia infrastruktury ogólnej w obiekcie spowodowane przez Wykonawcę podczas prowadzenia prac instalacyjnych obciążają jego samego i muszą być usunięte w ramach nieodpłatnego usunięcia szkód w terminie niezwłocznym po ich wykonaniu.

Zamawiający wymaga, aby odpady powstałe w wyniku realizowanych prac instalacyjnych, narzędzia i inne przedmioty były każdorazowo uprzątnięte z ciągów komunikacyjnych i z biur do godz. 7:00 rano tak aby umożliwiały bezpieczne wykonywanie pracy.

Wykonawca zobowiązany jest do pozostawienia pomieszczeń, w których będą wykonywane prace w stanie takim, jaki zastał przed przystąpieniem do prac.

1.3 AKTUALNE UWARUNKOWANIA WYKONANIA PRZEDMIOTU ZAMÓWIENIA

Prace montażowe będą wykonywane w lokalizacji Beskidzkiego Centrum Onkologii - Szpital Miejski przy ulicy Wyzwolenia 18 w Głównym Centrum Przetwarzania Danych (GCPD) oraz Zapasowym Centrum Przetwarzania Danych (ZCPD).

1.4 SZCZEGÓLNE UWARUNKOWANIA ZWIĄZANE Z WYKONANIEM ZAMÓWIENIA

Na terenie, gdzie będą wykonywane prace instalacyjno-montażowe znajduje się funkcjonująca instytucja lecznicza, która będzie użytkowana w trakcie realizacji Zamówienia.

Prowadzenie prac w trakcie pracy szpitala jest dozwolone w taki sposób, który nie będzie zakłócać jego funkcjonowania i prowadzić do dyskomfortu pracy pracowników oraz pacjentów Szpitala. Prace w tym okresie będą mogły być prowadzone po przekazaniu zasad wykonywania prac i zgody wydanej przez upoważnioną osobę ze strony Zamawiającego.

Dopuszcza się pracę w dni robocze w godzinach od 7:30 do 14:00. Wstęp, zasady poruszania i wykonywania prac w budynkach Szpitala przez pracowników Wykonawcy poza normalnymi godzinami pracy Szpitala będzie możliwy po przekazaniu zasad wykonywania prac w tym okresie i zgody wydanej przez upoważnioną osobę ze strony Zamawiającego.

Miejsca jak i urządzenia, w których Wykonawca będzie wykonywał prace, będą musiały być skutecznie zabezpieczone przed zabrudzeniem, zapyleniem, uszkodzeniem oraz zniszczeniem. Koszty związane potencjalnymi stratami w tym zakresie Wykonawca ponosi we własnym zakresie i jednocześnie zobowiązuje się, że stan Szpitala i zainstalowanych urządzeń nie będzie gorszy niż przed rozpoczęciem prac.

Wykonawca będzie przestrzegał wszystkich związanych z wykonywanymi pracami przepisów BHP.

Zamawiający będzie wymagał od wykonawcy na każdym etapie prac instalacyjnych w GCPD lub ZCPD szerokiej konsultacji dotyczącej terminu i sposobu realizacji etapu zadania, celem koordynacji z w celu zapewnienia ciągłości działania systemów informatycznych szpitala.

Dostarczone na miejsce budowy materiały należy sprawdzić pod względem ilości, kompletności i zgodności z danymi wytwórcy. Każdą dostawę towaru należy potwierdzić pisemnie.

Składowanie materiałów powinno odbywać się w warunkach zapobiegających zniszczeniu, uszkodzeniu lub pogorszeniu się właściwości technicznych na skutek wpływu czynników atmosferycznych lub

fizykochemicznych. Należy zachować wymagania wynikające ze specjalnych właściwości materiałów oraz wymagania w zakresie bezpieczeństwa przeciwpożarowego. Należy zastosować się do zaleceń producenta w w/w zakresie.

Informacje i dokumenty niezbędne do wykonania dokumentacji projektowej Wykonawca będzie ponosił wyłączną i pełną odpowiedzialność za treść dokumentacji projektowej, uzgodnione i własne założenia dokonane na potrzeby jej wykonania.

2. RÓWNOWAŻNOŚĆ ROZWIĄZAŃ

W celu zachowania reguły konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych w treści niniejszego OPZ, przy czym za rozwiązanie równoważne uważa się takie, które pod względem technologii, wydajności i funkcjonalności przez to rozwiązanie oferowanych, nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym.

Materiały lub urządzenia pochodzące od konkretnych producentów stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia. Pod pojęciem minimalne parametry jakościowe i cechy użytkowe Zamawiający rozumie wymagania dotyczące materiałów lub urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach pod względem:

a) gabarytów i konstrukcji (wielkość, rodzaj, właściwości fizyczne, liczba elementów składowych),
b) charakteru użytkowego (tożsamość funkcji),
c) charakterystyki materiałowej (rodzaj i jakość materiałów),
d) parametrów technicznych (wytrzymałość, trwałość, dane techniczne, dane hydrauliczne),
e) charakterystyki linowe, konstrukcja,
f) parametrów bezpieczeństwa użytkowania,
g) standardów emisyjnych.

W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób. Za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, identycznych dla obu rozwiązań, dla których to warunków rozwiązania te są dedykowane.

Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, iż spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.

3. GWARANCJA

Wykonawca udzieli 5-cio letniej gwarancji na przedmiot umowy, na warunkach zgodnie z wymaganiami określonymi w Opisie Przedmiotu Zamówienia, realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez linię telefoniczną producenta lub autoryzowanej firmy serwisującej.
Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia.

Urządzenia muszą być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, nieużywane przed dniem dostarczenia z wyłączeniem przeprowadzenia testu ich poprawnej pracy.

Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie kraju sprzedaży.

4. OZNACZENIE CE

Oferowane serwery muszą posiadać deklarację zgodności CE lub równoważną.

5. MINIMALNE WYMAGANIA DLA DOSTAW I USŁUG

5.1 WYMAGANIA OGÓLNE

Dla potrzeb Beskidzkiego Centrum Onkologii - Szpital Miejski im. Jana Pawła II w Bielsku Białej, Zamawiający wymaga dostawy oraz uruchomienia systemu wirtualizacji składającego się minimum z 2 kompletów serwerów. W ramach 1 kompletu serwerów dopuszcza się dostawę maksymalnie 2 urządzeń.

Zamawiający wymaga również dostawy oraz uruchomienia systemu WAF, który obejmie swym zakresem monitoring wszystkich usług informatycznych świadczonych przez Zamawiającego i udostępnianych do internetu.

Zamawiający wymaga w trakcie montażu wykonania minimum następujących czynności::

1. Zapoznanie z infrastrukturą Zamawiającego w Głównym Centrum Przetwarzania Danych – sześć szaf serwerowych – w celu ułożenia okablowania strukturalnego (zasilanie, LAN) dla istniejących urządzeń jak i dla nowych.
2. Rekonfiguracji środowiska wirtualizacji oVirt działającego u Zamawiającego w taki sposób aby nowe serwery były widoczne w systemie, była możliwość migracji online maszyn wirtualnych na nowe urządzenia, system umożliwiał budowania usług wysokiej dostępności (HA).
3. Rekonfiguracja środowiska wirtualizacji oVirt działającego u Zamawiającego uwzględniająca położenie serwerów w GCPD (Głównym Centrum Przetwarzania Danych), ZCPD (Zapasowym Centrum Przetwarzania Danych) zapewniające ciągłość działania w przypadku awarii jednego z Centrów Danych. Rekonfiguracja musi obejmować również rekonfigurację replikacji danych macierzowych w celu zapewnienia spójności danych.

4. Rekonfiguracja systemu monitoringu infrastruktury Zabbix w zakresie co najmniej takim, że system będzie nadzorował działanie nowo dostarczonych urządzeń zbierając informacje o ich pracy oraz wysyłał alerty na ustalony adres e-mail o nieprawidłowościach działania. Alert maja obejmować co najmniej informację o uszkodzeniu, któregoś z elementów – zasilacz, procesor, pamięć, dysk twardy, karat sieciowa – oraz barku dostępności usług świadczonych przez oprogramowanie zainstalowane na tych urządzeniach.
   W ramach rekonfiguracji należy również skonfigurować monitoring innych wskazanych przez Zamawiającego systemów wirtualizowanych które będą migrowane na nowo zakupione urządzenia
5. Rekonfiguracji systemu backupu według ustalonego w projekcie harmonogramu i przygotowanego projektu tak aby zapewnić backup konfiguracji oraz danych zebranych przez dostarczone urządzenia.

5.2 WYMAGANIA DLA SERWERÓW – 2 KOMPLETY

Nazwa komponentu	Wymagania minimalne dotyczące 1 kompletu.
Budowa	Obudowa RACK 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w oferowanej szafie). Kompletny serwer nie może składać się więcej niż z 2 części fizycznych.
Procesor	Zainstalowane min. cztery procesory po 32 rdzenie o szybkości podstawowej min. 3,3 Ghz osiągające w teście https://www.cpubenchmark.net min. 78000 pkt. Obsługujące standard PCIe 5.0
RAM	Min. 24 gniazda DDR5 DIMM (12 gniazd DIMM na procesor). Każdy procesor posiada min. 12 kanałów pamięci, 1 moduł DIMM na kanał. Zainstalowane min. 1024 GB DDR5 4800MHz–. Możliwość rozbudowy do min. 12 TB z 48 modułami 3DS RDIMM o pojemności 256GB.
Pamięć dyskowa	Serwer musi obsługiwać min. 4 3,5-calowe wnęk na dyski typu hot-swap. Zainstalowane cztery dysk M.2, każdy min. 960GB NVMe PCIe SSD. Możliwość rozbudowy i instalacji min. 24 dysków typu hot-swap 2,5-calowych NVMe SSD, SAS, SATA.
Interfejsy sieciowe	• Dedykowane gniazdo OCP 3.0 z interfejsem hosta PCIe Gen. 5 x16. • Zainstalowana karta 2-portowa SFP+ z łącznością sieciową 10GbE/25GbE. • Zainstalowana karta 16Gb Gen6 FC Dual-port HBA
Karta graficzna	• Min. 16 MB pamięci z akceleratorem sprzętowym 2D. • Min. rozdzielczość 1920x1200 32bpp przy 60Hz.
Gniazda PCI	Min, 2 gniazda PCIe Gen 5 + 1 gniazdo PCIe Gen 4. Dodatkowe gniazdo OCP 3.0.
Kontrolery	• Wbudowany NVMe — min. 24 dysków, każdy x4 • Wbudowane złącze SATA — min. 24 dysków
Porty	• Przód: min. 1x port USB 3.1 G1 (5 Gb/s), min. 1x port USB 2.0, zewnętrzny port diagnostyczny, opcjonalny port VGA. • Tył: min. 3x porty USB 3.1 G1 (5 Gb/s), min. 1x port wideo VGA, 1x port zarządzania systemami RJ-45 1GbE do zdalnego zarządzania. • Wewnętrzne: min. 1x złącze USB 3.1 G1 na potrzeby systemu operacyjnego lub klucza licencyjnego.

Chłodzenie	8 nadmiarowych wentylatorów N+1 z możliwością wymiany podczas pracy. Jeden wentylator zintegrowany z każdym zasilaczem. Jeden wentylator zintegrowany w każdym zasilaczu. Radiator chłodzony cieczą w zamkniętej pętli do chłodzenia procesorów.
Inne	• Dwa redundantne zasilacze. • Możliwość wymiany uszkodzonych elementów przy pracy urządzenia - napędy, zasilacze i wentylatory. • Panel operatora z diodami LED stanu. Wbudowane zarządzanie zaawansowane / zdalna graficzna konsola użytkownika HTML5. • Czujnik naruszenia obudowy, hasło włączenia, hasło administratora, moduł Trusted Platform Module (TPM), obsługujący TPM 2.0 i Platform Firmware Resiliency (PFR). • Obsługiwane systemy operacyjne min. Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi. • Min 5-cio letnia gwarancja. Przyjmowanie zgłoszeń 24/7/356. Naprawa NBD.

5.3 WYMAGANIA DLA WEB APLICATION FIREWALL

System ochrony aplikacji webowych oraz Firewall XML, którego zadaniem będzie wykrywanie i blokowanie ataków celujących w aplikacje webowe a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. Powinien zostać dostarczony w postaci komercyjnej platformy instalowanej w środowisku wirtualnym: VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, Oracle Cloud. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych w ww środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić niezbędny odpowiednio zabezpieczony systemem operacyjny.

Środowisko eCareMed w przedmiotowym zakresie bazuje na rozwiązaniach Web Application Firewall o następujących parametrach funkcjonalnych:

- Wsparcie dla min. 5 serwerów obsługiwanych przez WAF (tzw. backend)
- Wydajność min. 100 Mbps,
- Wydajność transakcji HTTPS/SSL – min. 1000/sek,
- Ochrona aplikacji internetowych w zakresie OWASP Top 10
- Geo-IP i reputacja IP (w tym publiczne serwery proxy i węzły Tor)
- Ochrona przed kradzieżą danych wychodzących (Karty kredytowe, PESEL, SSN itp.)
- Kontrola wgrywanych plików
- Zabezpieczenia wgrywanych plików (antywirus i Zaawansowana ochrona przed zagrożeniami)
- Maskowanie strony internetowej
- Kontrola protokołu dla ruchu HTTP i HTTPS
- Szczegółowe zasady dotyczące poszczególnych adresów URL/parametrów
- Kontrola ilości zapytań
- Monitoring „życia” backend serwera poprzez cykliczne wysyłanie żądań do aplikacji, pakiety icmp,
- Ochrona API w zakresie OWASP Top 10
- Bezpieczeństwo interfejsu API (JSON)
- Bezpieczeństwo API (XML)
- Wykrywanie API (JSON)
- Wykrywanie API (XML)

- Ochrona przed skanowaniem stron internetowych, w tym Baza danych znanych botów
- Ochrona przed spamem botów
- Ochrona przed spamem formularzy
- Ochrona przed wstrzykiwaniem poświadczeń
- Ochrona przed atakami Brute Force
- Obsługa CAPTCHA (wewnętrzna, reCAPTCHA v2 i v3)
- Ochrona aplikacji przed atakami DDoS
- TLS/SSL Offloading
- Równoważenie obciążenia i routing zawartości
- Dynamiczne szyfrowanie adresu URL
- Obsługa protokołów HTTP/1.0, HTTP/1.1, HTTP/2.0, WebSocket, FTP/S i IPv6
- Kontrola żądań i odpowiedzi (tłumaczenie adresów URL)
- Buforowanie i kompresja
- Lokalni użytkownicy/grupy (wewnętrzny LDAP), Certyfikaty klienta
- Wsparcie dla LDAP/Active Directory, RADIUS, Kerberos v5, kody dostępu SMS,
- Jedno- i wielodomenowe logowanie jednokrotne
- Usługa Przeciwdziałania zagrożeniom dostarczana przez producenta rozwiązania
- Obsługa implementowania zabezpieczeń dla przynajmniej 8 znanych skanerów podatności
- Wbudowane logowanie (min, dzienniki dostępu, dzienniki audytu, dzienniki zapory sieciowej i dzienniki systemowe)
- Raportowanie na żądanie i zaplanowane z możliwością customizacji raportów
- Możliwość wykorzystania zewnętrznego SysLoga
- Sieciowe listy ACL
- Dodatkowa Zaawansowana ochrona przed botami w trybie subskrypcji
- Dodatkowa Zaawansowana ochrona przed zagrożeniami w trybie subskrypcji.
- Kontrola antywirusowa dla komunikacji http realizowana na firewall'u aplikacyjnym lub zewnętrznym systemie w oparciu o protokół icap. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
- W ramach postępowania wymaganym jest dostarczenie licencji upoważniającej do współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
- System musi pozwalać na weryfikacje nazwy użytkownika i hasła w ramach mechanizmów ochrony przed Credential Stuffing. W ramach postepowania muszą zostać dostarczone niezbędne do uruchomienia tej funkcji licencje.

Z uwagi na złożoną architekturę aplikacji zabezpieczanych przez WAF, związaną między innymi z wykorzystywaniem autentykacji poprzez certyfikaty zastosowane rozwiązanie musi zapewniać zaawansowane mechanizmy analizy i ochrony aplikacji web, mechanizmy monitoringu i inspekcji oraz tworzenia profilów aplikacji na podstawie analizy zapytań kierowanych do kontentu backend. Ze względu na wielość lokalizacji, w których serwowana jest aplikacja rozwiązanie musi zapewniać możliwość tworzenia szablonów polityk bezpieczeństwa i łatwej ich dystrybucji pomiędzy urządzeniami w pozostałych lokalizacjach. W ramach wdrożenia konieczna jest uruchomienie oraz z komunikowanie z platformą

regionalną eCareMed oraz dostosowanie dostarczonego rozwiązania WAF zgodnie wytycznymi zawartymi w załączniku nr 1- Założenia do warstwy komunikacyjnej Platformy Regionalnej w punkcie 2 dokumentu .