Zielona Góra, dnia 10/11/2022 r.

Zamawiający:
Samodzielny Publiczny Zakład Opieki Zdrowotnej
Ministerstwa Spraw Wewnętrznych i Administracji
w Zielonej Górze

WYJAŚNIENIA ORAZ ZMIANA SWZ

Dotyczy: Dostawa komputerów oraz serwerów" - nr postępowania: ZP/08/2022.

Zamawiający informuje, iż w przedmiotowym postępowaniu wpłynął wniosek o wyjaśnienie treści Specyfikacji Warunków Zamówienia (dalej: SWZ). Zamawiający na podstawie art. 284 ust. 6 ustawy z dnia 11 września 2019 roku – Prawo zamówień publicznych (dalej: ustawa PZP) udostępnia treść zapytań wraz z wyjaśnieniami.

Pytanie nr 1
Załącznik nr 5 do SWZ – OPZ, Serwer
Czy Zmawiający potwierdza, że szafa rack, klimatyzator ścienny 3,5 kW; UPS typu 5PX 2200i RT2U Netpack G2; kamera IP min 4 Mpix oraz UTM Firewall typ FG-40F nie są elementami składowymi serwerów i nie podlegają gwarancji wskazanej dla serwerów?
Prosimy o usunięcie z opisu serwera tych dodatkowych elementów.
Odpowiedź: Zamawiający potwierdza, zgodnie ze zmianami w OPZ.

Pytanie nr 2
Załącznik nr 5 do SWZ – OPZ
Czy Zamawiający uzna za spełnienie wymagań dostarczenie szafy rack o następujących parametrach?

Szerokość	19"
Wysokość	27U
Szerokość zewnętrzna	600 mm
Głębokość zewnętrzna	1000 mm
Konstrukcja ramy	Skręcana
Drzwi przednie	przeszklone - zamykane na klucz
Drzwi tylne	stalowe perforowane - zamykane na klucz
Osłony boczne	stalowe - zamykane na klucz
Gwarancja	Min 24 miesiące

Odpowiedź: Zamawiający dopuszcza.

Pytanie nr 3
Załącznik nr 5 do SWZ – OPZ
Czy Zamawiający uzna za spełnienie wymagań dostarczenie klimatyzatora ściennego o następujących parametrach?

Wydajność chłodzenia (min/norm/max	0,90/3,20/3,60 kW
Wydajność grzania (min/norm/max	0,90/3,40/4,00 kW
Pobór mocy (min/nom/max)	Chłodzenie - 0,22/0,99/1,30 kW; Grzanie - 0,22/0,92/1,50 kW
Klasa sezonowej efektywności energetycznej	Chłodzenia - A++; Grzanie - A+
Pobór prądu (wartość nominalna)	Chłodzenie 4,4A; Grzanie 4A
Gwarancja	36 miesięcy (w cenie oferty należy uwzględnić wymagane przeglądy okresowe oraz montaż) - Skropliny odprowadzone na zewnątrz grawitacyjnie (bez użycia pompek skroplin) – długość instalacji max 8m - zasilanie z najbliższego gniazdka elektrycznego

Odpowiedź: Zamawiający dopuszcza.

Pytanie nr 4

Załącznik nr 5 do SWZ – OPZ

Czy Zamawiający uzna za spełnienie wymagań dostarczenie zasilacza UPS o następujących parametrach?

Moc pozorna	2200 VA
Moc rzeczywista	2200 W
Topologia (klasyfikacja IEC 62040-3)	Line-interactive z AVR
Współczynnik mocy	1
Czas przełączenia na baterię	<4 ms
Liczba, typ gniazd wyjściowych	8 x IEC C13 (2 grupy po 2 gniazda IEC C13 gniazd sterowalnych za pomocą oprogramowania oraz z poziomu wyświetlacza), 1 x IEC C19 16A
Typ gniazda wejściowego	IEC C20 16A
Czas podtrzymania dla 100% obciążenia dla pf=1	3 min
Czas podtrzymania przy 50% obciążenia dla pf=1	10 min
Napięcie znamionowe	200/208/220/230/240 V
Tolerancja napięci prostownika	160 V – 294 V (regulacja programowa 150-294 V)
Częstotliwość znamionowa	50/60 Hz autodetekcja

Tolerancja częstotliwości	47– 70 Hz, 40 Hz w trybie niskiej czułości
Kształt napięcia	Sinusoidalny
Napięcie znamionowe wyjściowe	200/208/220230/240 V do wyboru przez użytkownika
Zakres zmian napięcia	+6/-10% napięcia nominalnego
Częstotliwość wyjściowa	50/60 Hz

Czas ładowania baterii do poziomu 90%	< 3 godz. do 90% pojemności użytkowej
Interfejs komunikacyjny	• USB • RS232 DB-9 żeński (HID) • styki przekaźnikowe • miniport wyłącznik ON/OFF • SNMP/Ethernet
Panel sterowania z wyświetlaczem LCD	Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o: stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe, częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny, napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii w kWh).
Sygnały akustyczne	• Awaria • Niski stan naładowania baterii • Przeciążenie • Serwis
Dane techniczne karty SNMP	Network Support: Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex / HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP/ Protokoły: MQTT/RNDIS/LDAP/NVD/SSH/PKI Kamptybilność: SNMP v1/v3 i IP v4/v6 Interfejs: HTML5 Adresowanie IP: DHCP/BootP/Manualne Szyfrowanie: pakiet szyfrów TLS 1.2 z minimum SHA256 Dostępny port USB (microUSB - port serwisowy) Certyfikaty: CA, UL 2900-1, 2900-2-2

Dołączone oprogramowanie	Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie serwerów zasilanych z systemu i pracujących pod kontrolą systemów operacyjnych: - Windows: 7 / 8 / 2008 / Vista / 2003 / XP - Microsoft SCVMM 2012 - Linux: Debian GNU Linux: Lenny, SUSE/Novell: SLES 11, OpenSUSE 11.2, Redhat Enterprise Linux: RHEL 5.3, 5.4, 5.5, Fedora core 12 Ubuntu: 10.04 - VMWare: vCenter / ESXi 5.1 - Citrix XEN 6.0
Znaki bezpieczeństwa	CE, TUV, CB Report, IEC/EN 62040-1-1, IEC/EN 62040-2
Gwarancja	60 miesięcy na urządzenie i akumulatory

Odpowiedź: Zamawiający dopuszcza.

Pytanie nr 5

Załącznik nr 5 do SWZ – OPZ

Czy Zamawiający uzna za spełnienie wymagań dostarczenie kamery IP o następujących parametrach?

Sensor:	1/2.7” 4MP Progressive CMOS
Rozdzielczość:	2560 x 1440
Ogniskowa:	3.6 mm
Pole widzenia:	92°(H), 48°(V), 119°(D) 355° obrotu, -5-80° nachylenia
Łączność sieciowa	Wi-Fi: IEEE 802.11 b/g/n
Pozostałe	Slot karty MicroSD (w komplecie należy dostarczyć kartę microSD min. 128 GB)
Kompresja wideo:	H.265/H.264
Ochrona	Detekcja ruchu Konfiguracja obszaru ochrony Rozróżnianie obiektów (Detekcja osób; Human Detection)
Gwarancja	min 24 miesiące

Odpowiedź: Zamawiający dopuszcza.

Pytanie nr 6

Załącznik nr 5 do SWZ – OPZ

Czy Zamawiający uzna za spełnienie wymagań dostarczenie urządzenia UTM o następujących parametrach?

Wymagania Ogólne	System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie:	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 5 portami Gigabit Ethernet RJ-45. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

Parametry wydajnościowe:	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Funkcje Systemu Bezpieczeństwa:	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.

Kontrola WWW	1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Certyfikaty	Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.
Gwarancja oraz wsparcie	1. Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement).

Odpowiedź: Zamawiający dopuszcza.

Pytanie nr 7

Załącznik nr 3 do SWZ – Wzór umowy, par. 8 ust. 1

Prosimy o modyfikację par. 8 ust. 1 w taki sposób, aby możliwe było wpisanie odrębnych okresów gwarancyjnych dla poszczególnych urządzeń, które będą miały różne okresy gwarancji.

Odpowiedź: Zamawiający dokonuje modyfikacji w zakresie § 8 ust. 1. W związku z powyższym Zamawiający zamieszcza na stronie internetowej prowadzonego postępowania zmodyfikowany załącznik nr 3 – Wzór umowy po zmianach.

Pytanie nr 8

Załącznik nr 3 do SWZ – Wzór umowy, par. 8 ust. 2

Czy Zamawiający potwierdzi, że zapisy par. 8 ust. 2 dotyczą tylko serwerów? Zwracamy uwagę, iż producenci pozostałego sprzętu dostarczanego w ramach tego postępowania nie zapewniają takich warunków gwarancyjnych dla swoich produktów.

Odpowiedź: Zgodnie z SWZ.

Pytanie nr 9

Załącznik nr 3 do SWZ – Wzór umowy, par. 1 ust. 1

Zwracamy uwagę, że w ramach przewidzianej przedmiotem zamówienia migracji najprawdopodobniej dochodzić będzie do przetwarzania danych osobowych w ramach powierzenia ich Wykonawcy jako podmiotowi przetwarzającemu przez Zamawiającego jako administratora. Migracja danych w systemach informatycznych zaś to proces dalece wyspecjalizowany, którego wykonawca kieruje się wypracowanymi i utrwalonymi metodami i procedurami, w tym obejmującymi przetwarzanie powierzonych mu danych osobowych. Owo przetwarzanie i zgodne z prawem reguły nim rządzące każdy z takich wykonawców zapisał w stosowanych przez siebie wzorcach umów, regulaminach, których stosowanie daje gwarancje, że dane osobowe w toku migracji wykonywanej przez danego wykonawcę będą właściwie zabezpieczone i chronione, a co za tym idzie, że nie dojdzie do ich naruszenia. Tym samym czy Zamawiający potwierdzi, że w przypadku, gdy w ramach realizacji zamówienia konieczne stanie się powierzenie Wykonawcy danych osobowych administrowanych przez Zamawiającego, zaakceptuje on ich przetwarzanie przez tegoż Wykonawcę w oparciu o regulamin przetwarzania danych osobowych wdrożony w przedsiębiorstwie Wykonawcy, wcześniej Zamawiającemu udostępniony?

Odpowiedź: Tak.

Pytanie nr 10

Załącznik nr 3 do SWZ – Wzór umowy, par. 6 ust. 5

Zwracamy uwagę, że to postanowienie wzoru umowy jest szczególnie niekorzystne dla Wykonawcy, gdyż wymusza na nim złożenie niekorzystnego dla niego oświadczenia woli, a poza tym wyklucza Wykonawcy jakąkolwiek możliwość obrony przed niesłusznym obciążeniem go przez Zamawiającego karami umownymi. Tym samym, to Zamawiający zyskuje wyłączne prawo do swobodnego i nieuzasadnionego naliczania Wykonawcy kar umownych, co stawia go jako podmiot nadrzędny nad Wykonawcą, co zaś wprost zaprzecza zasadzie równości stron umowy cywilnoprawnej, którą zgodnie z prawem zamówień publicznych jest umowa na wykonanie zamówienia publicznego. Tym samym, aby doprowadzić wzór umowy do powszechnie uznanych i obowiązujących zasad prawa cywilnego, które nie są krzywdzące dla żadnej ze stron, jak to właśnie postanowienie jest krzywdzące dla Wykonawcy, prosimy o wykreślenie z par. 6 wzoru umowy ust. 5 w całości.

Odpowiedź: Zgodnie z SWZ.

Pytanie nr 11

Załącznik nr 3 do SWZ – Wzór umowy, par. 8 ust. 2

Czy Zamawiający potwierdzi, że dniami roboczymi w rozumieniu tego postanowienia wzoru umowy są dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy?

Odpowiedź: Tak

Z uwagi na powyższe Zamawiający na podstawie art. 286 ust. 1 w związku z art. 284 ust. 3 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych przedłuża termin składania ofert i dokonuje zmiany treści Specyfikacji Warunków Zamówienia (dalej: SWZ).

ZMIANA TREŚCI SPECYFIKACJI WARUNKÓW ZAMÓWIENIA

nastąpiła w następującym zakresie i miejscu:

ROZDZIAŁ XIII SPOSÓB ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT, TERMIN ZWIĄZANIA OFERTĄ

13.1. Ofertę należy złożyć za pośrednictwem Formularza do złożenia, zmiany, wycofania oferty lub wniosku dostępnego na e-PUAP i udostępnionego na miniPortalu, **do dnia 15.11.2022 r., godz. 10:00.**

13.2. Otwarcie ofert nastąpi w **dniu 15.11.2022 r. o godz. 10:15.**

13.7. Wykonawca związany jest ofertą przez 30 dni od dnia upływu terminu składania ofert tj. **do dnia 14.12.2022 r.** Pierwszym dniem terminu związania ofertą jest dzień, w którym upływa termin składania ofert.

Zamawiający informuje, że powyższe wyjaśnienia i zmiana stanowią integralną część SWZ i są wiążące dla wszystkich Wykonawców biorących udział w postępowaniu o udzielenie zamówienia.