#### PAKIET 1

#### *6.1.6.3   Wymagania minimalne dotyczące skanera małego*

####

#### 1.     Zamawiający określił parametr: Rozdzielczość wyjściowa min. od 50 do 600 dpi. Dla prawidłowego podziału skanowanych pism na dokumenty systemy klasy EZD wykorzystują kody kreskowe. Skuteczność rozpoznania kodów oraz treści skanowanych obrazów przy tak niskiej rozdzielczości jest niemożliwa do osiągnięcia, dlatego też wnosimy o zmianę tego parametru na:

#### Rozdzielczość wyjściowa: minimum 100 do 600 DPI.

#### Zamawiający nie określił nigdzie w SIWZ, że będzie skanował kody kreskowe w rozdzielczości 50dpi. Podtrzymuje zapis w SIWZ.

#### 2.     Zamawiający określił parametr: Rozmiar dokumentów min. 50 mm x 50 mm. Zapis ten wskazuje tylko na jednego producenta skanerów dokumentowych jakim jest Avision. Zamawiający dokonał opisu parametrów technicznych w sposób utrudniający uczciwą konkurencję pomiędzy wykonawcami, co jest niedopuszczalne w świetle art. 29 ust. 2 Ustawy. Ten parametr spełnia tylko jeden producent – Avision. W związku z tym wnosimy o zmianę tego parametru na:

#### Rozmiar dokumentów min. 52 mm x 52 mm, Maks. 216 mm x 356 mm

#### Zamawiający zmienia minimalne rozmiary skanowanego dokumentu z 50mm x 50mm na nie większe niż 81mm x 81mm.

3.     Zamawiający określił parametr: Prędkość skanowania  min. 30 PPM / 60 IPM (dla: kolor, B&W, A4, 300 dpi), min. 40 PPM / 80 IPM (dla: kolor, B&W, A4, 200 dpi).

Wysoka jakość skanów, odczyt kodów kreskowych oraz skuteczność rozpoznania OCR wymaga użycia trybu czarno białego i  rozdzielczości 300 DPI. Powyższy zapis spełnia tylko jeden producent jakim jest Avision.

W związku z tym wnosimy o zmianę tego parametru na: min. 40 PPM / 80 IPM (dla: kolor, B&W, A4, 300 dpi)

Prędkość skanowania przy rozdzielczości 200 dpi jest większa niż przy rozdzielczości 300 dpi, zatem jeżeli sprzęt Wykonawcy zapewnia większą prędkość skanowania przy rozdzielczości 200 dpi lub zapewnia tą prędkość przy większym niż 200 dpi, parametr zostanie spełniony. Zamawiający podtrzymuje zapis SIWZ.

4.     Zamawiający określił parametr: Sugerowana obciążalność dzienna 5000 stron.

Prosimy o doprecyzowanie tego parametru, czy Zamawiający ma na myśli 5000 stron w co odpowiada 2 500 arkuszy dziennie w trybie duplex czy 5000 fizycznych arkuszy.

Parametr został wyraźnie określony jako „STRON”. Zatem wymagania spełnia skaner zapewniający obciążalność dzienną większą bądź równą skanowaniu 5000 arkuszy papieru jednostronnie [czyli 5000 stron] oraz taki który zapewnia 2500 arkuszy w trybie dwustronnym [czyli 5000 stron].

5.     Zamawiający określił parametr: Interfejs min. USB 2.0

Od wielu lat standardem komunikacyjnym dla skanerów dokumentowych jest USB 3.0, wszystkie nowoczesne stacje robocze oraz laptopy są wyposażone w kilka takich portów. Nowy interfejs jest dużo szybszy i gwarantuje błyskawiczny transfer dokumentów ze skanera do stacji roboczej bez spowolnienia skanowania.

Wnosimy o zmianę tego parametru na: Interfejs min. USB 3.0 kompatybilny z USB 2.0

Interface w standardzie USB 3.0 spełnia warunki minimalne zapisów SIWZ. Zamawiający podtrzymuje zapis SIWZ.

#### *6.1.6.4   Wymagania minimalne dotyczące skanera dużego*

####

#### 6.     Zamawiający określił parametr: Rozdzielczość wyjściowa min. od 50 do 600 dpi. Dla prawidłowego podziału skanowanych pism na dokumenty systemy klasy EZD wykorzystują kody kreskowe.Skuteczność rozpoznania kodów oraz treści skanowanych obrazów przy tak niskiej rozdzielczości jest niemożliwa do osiągnięcia, dlatego też wnosimy o zmianę tego parametru na:

#### Rozdzielczość wyjściowa: minimum 100 do 600 DPI.

#### Zamawiający nie określił nigdzie w SIWZ, że będzie skanował kody kreskowe w rozdzielczości 50dpi. Podtrzymuje zapis SIWZ.

#### 7.     Zamawiający określił parametr: Rozmiar dokumentów min. 50 mm x 50 mm. Zapis ten wskazuje tylko na jednego producenta skanerów dokumentowych jakim jest Avision. Zamawiający dokonał opisu parametrów technicznych w sposób utrudniający uczciwą konkurencję pomiędzy wykonawcami, co jest niedopuszczalne w świetle art. 29 ust. 2 Ustawy. Ten parametr spełnia tylko jeden producent – Avision. W związku z tym wnosimy o zmianę tego parametru na:

#### Rozmiar dokumentów min. 52 mm x 52 mm, Maks. 216 mm x 356 mm

#### Zamawiający zmienia minimalne rozmiary skanowanego dokumentu z 50mm x 50mm na nie większe niż 81mm x 81mm.

8.     Zamawiający określił parametr: Prędkość skanowania  min. 40 PPM / 80 IPM (dla: kolor, B&W, A4, 300 dpi), min. 60 PPM / 120 IPM (dla: kolor, B&W, A4, 200 dpi).

Wysoka jakość skanów, odczyt kodów kreskowych oraz skuteczność rozpoznania OCR wymaga użycia trybu czarno białego i  rozdzielczości 300 DPI. Powyższy zapis spełnia tylko jeden producent jakim jest Avision.

W związku z tym wnosimy o zmianę tego parametru na: min. 60 PPM / 120 IPM (dla: kolor, B&W, A4, 300 dpi)

Prędkość skanowania przy rozdzielczości 200 dpi jest większa niż przy rozdzielczości 300 dpi, zatem jeżeli sprzęt Wykonawcy zapewnia większą prędkość skanowania przy rozdzielczości 200 dpi lub zapewnia tą prędkość przy większym niż 200 dpi, parametr zostanie spełniony. Zamawiający podtrzymuje zapis SIWZ.

9.     Zamawiający określił parametr: Sugerowana obciążalność dzienna 5000 stron.

Prosimy o doprecyzowanie tego parametru, czy Zamawiający ma na myśli 5000 stron w co odpowiada 2 500 arkuszy dziennie w trybie duplex czy 5000 fizycznych arkuszy.

Parametr został wyraźnie określony jako „STRON”. Zatem wymagania spełnia skaner zapewniający obciążalność dzienną większą bądź równą skanowaniu 5000 arkuszy papieru jednostronnie [czyli 5000 stron] oraz taki który zapewnia 2500 arkuszy w trybie dwustronnym [czyli 5000 stron].

10.  Zamawiający określił parametr: Interfejs min. USB 2.0

Od wielu lat standardem komunikacyjnym dla skanerów dokumentowych jest USB 3.0, wszystkie nowoczesne stacje robocze oraz laptopy są wyposażone w kilka takich portów. Nowy interfejs jest dużo szybszy i gwarantuje błyskawiczny transfer dokumentów ze skanera do stacji roboczej bez spowolnienia skanowania.

Wnosimy o zmianę tego parametru na: Interfejs min. USB 3.0 kompatybilny z USB 2.0

Interface w standardzie USB 3.0 spełnia warunki minimalne zapisów SIWZ. Zamawiający podtrzymuje zapis SIWZ.

PAKIET 2

1. Dotyczy SIWZ, Rozdział V, ust. 1, pkt 2), ppkt I, lit b).
2. Zamawiający wymaga, aby: *„Wykonawca w każdym roku działalności posiadał minimalny roczny obrót w wysokości minimum 9 000 000 zł, w tym minimalny roczny obrót w obszarze objętym zamówieniem (związany z działalnością związaną z dostawą i wdrożeniem systemów informatycznych, w tym: zaprojektowaniem, wytwarzaniem i instalacją oprogramowania) w wysokości minimum 6 000 000 zł.”*

Jednocześnie dalej Zamawiający wyjaśnia, że: *„Na podstawie art. 22c ust. 1 pkt. 1) i ust. 2 Zamawiający informuje, że wymóg ten jest pochodną szacunkowej wartości zamówienia, czasu jego realizacji. Zamawiający zakłada, z uwzględnieniem dwunastomiesięcznego okresu realizacji zamówienia, że ubiegać się o niniejsze zamówienie może tylko wykonawca, który wykaże łączny roczny obrót w obszarze objętym zamówieniem w wysokości 9.000.000 zł.”*

Zatem w treści samego warunku udziału w postępowaniu Zamawiający wymaga wykazania się minimalnym rocznym obrotem w obszarze objętym zamówieniem na poziomie minimum 6 000 000,00 zł, a w komentarzu do warunku wymaga już obrotu w tym samym zakresie na poziomie 9 000 000,00 zł. Prosimy o wyjaśnienie, która z kwot jest prawidłowa oraz o ujednolicenie treści SIWZ w tym zakresie.

Zapis w SIWZ jest omyłką pisarską – Zamawiający poprawił zapis w SIWZ z 9 000 000 na 6 000 000.

1. Prosimy o potwierdzenie, że Zamawiający nie wymaga na potwierdzenie spełniania warunków opisanych w SIWZ Rozdział V, ust. 1, pkt 2), ppkt I, lit a) i b) składania jakichkolwiek dokumentów, a jedynie wymaga potwierdzenia spełniania tych warunków w ramach składanego Jednolitego Europejskiego Dokumentu Zamówienia. Katalog dokumentów składanych na potwierdzenie spełniania warunków udziału w postępowaniu (Rozdział VII, ust. 5) nie zawiera wymogu składania dokumentów potwierdzających spełnianie opisanych warunków udziału.

Zamawiający potwierdza, że nie wymaga na potwierdzenie spełniania warunków opisanych w SIWZ Rozdział V, ust. 1, pkt 2), ppkt I, lit a) i b) składania jakichkolwiek dokumentów, a jedynie wymaga potwierdzenia spełniania tych warunków w ramach składanego Jednolitego Europejskiego Dokumentu Zamówienia. Dokumenty wymienione w Rozdziale VII dostarczy Wykonawca, którego oferta zostałą wybrana jako najkorzystniejsza.

1. Dotyczy SIWZ, Rozdział V, ust. 1, pkt 2), ppkt II, lit a), b), c).

Prosimy o wyjaśnienie, czy podane w warunkach kwoty są kwotami netto czy brutto.

Podane w warunkach kwoty są kwotami brutto.

1. Dotyczy SIWZ, Rozdział VII, ust. 5, pkt 8) oraz Załącznik nr 10 do SIWZ – wykaz dostaw.

Prosimy o wyjaśnienie, w jakim celu Zamawiający umieścił wśród dokumentów postępowania Załącznik nr 10 – wykaz dostaw. Zgodnie z treścią Rozdziału VII SIWZ, ust. 5, pkt 8) Zamawiający wymaga, aby w celu potwierdzenia spełniania warunków udziału w postepowaniu Wykonawca złożył wykaz wykonanych usług – Załącznik nr 5 do SIWZ. Nigdzie w treści SIWZ Zamawiający nie wymaga złożenia Załącznika nr 10 do SIWZ.

Zamawiający zmienił zapis SIWZ w tym zakresie.

1. Dotyczy SIWZ, Rozdział VIII, ust. 6.

Prosimy o potwierdzenie, że zapis jest omyłką pisarską, albowiem w postępowaniach
o wartości przekraczającej kwoty określone w przepisach wydanych na podstawie art. 11 ust. 8 ustawy Pzp, Zamawiający zobowiązany jest udzielić odpowiedzi na pytania Wykonawców nie później niż na 6 dni przed upływem terminu składania ofert.

Zamawiający potwierdza, że jest to omyłka pisarska. Zamawiający zmienił zapis SIWZ w tym zakresie.

1. Dotyczy SIWZ, Rozdział XIII, ust. 6.

Zgodnie z informacją podana przez Zamawiającego, w ramach kryterium oceny bezpieczeństwa systemu można uzyskać maksymalnie 18 punktów. Tymczasem po zsumowaniu maksymalnych wartość punktacji w poszczególnych podkryteriach (lit a) – 6 pkt, lit b) opcja D – 4 pkt, lit c) opcja B – 5 pkt) otrzymujemy wynik równy 15 punktów. Prosimy o wyjaśnienie (ewentualne usunięcie) rozbieżności zapisów.

Pkt 6 otrzymuje brzmienie:

* 1. „Wartość punktowa w kryterium oceny systemu bezpieczeństwa będzie przyznawana wg. poniższego wzoru:
1. Zmniejszenie procentowe [do max 50%] czasów usunięcia Dysfunkcji zawartych w warunkach SLA – Załącznik nr 6 do Umowy – maks. 8 pkt.:

$$Wp3a=oferowany poziom obniżenia czasu w \%\* \frac{waga punktowa (6)}{maksymalny poziom obniżenia czasu (50)}$$

1. bezpieczeństwo lokalnych systemów:

A – backup ręczny danych wykonywany przez operatora Wykonawcy – 0 pkt

B – backup wykonywany przez skrypty [np.: bash, powershell, itp.] zapisujące dane na dyskach lokalnych wirtualnych maszyn i w lokalizacji centralnej – 1 pkt.

C – backup automatyczny danych zawartych na wirtualnych maszynach z użyciem dedykowanego systemu do backupu – 2 pkt.

D – backup automatyczny zarówno całych maszyn wirtualnych jak i danych zawartych na tych maszynach z użyciem dedykowanego systemu do backupu i dedykowanych wirtualnych maszyn w lokalizacjach terenowych – 5 pkt.

1. bezpieczeństwo systemów chmurowych:

A – zapewnienie bezpieczeństwa usług na poziomie minimalnym wymaganym przez SzOPZ - 0 pkt

B – zapewnienie rozwiązań HA w trybie Active-Active dla wszystkich zasobów i usług w lokalizacji centralnej - 5 pkt

Punkty otrzymane w ppkt. a), b) i c) zostaną zsumowane. Maksymalna ilość punktów do zdobycia w powyższym kryterium wynosi 18 pkt.

”

1. Dotyczy SIWZ, Rozdział XIII, ust. 7.

Zgodnie z informacją podana przez Zamawiającego, w ramach kryterium oceny dodatkowych miesięcy gwarancji można uzyskać maksymalnie 13 punktów. Tymczasem po zsumowaniu wag punktowych dla poszczególnych urządzeń otrzymujemy wynik równy 12 punktów. Prosimy o wyjaśnienie (ewentualne usunięcie) rozbieżności zapisów.

Wagi punktowe w pkt 7 otrzymują brzmienie:

„Wagi punktowe dla:

1. serwerów: 3 pkt.
2. macierzy: 3 pkt.
3. przełączników: 2 pkt.
4. routerów: 2 pkt.
5. komputerów: 1 pkt.
6. drukarek: 1 pkt.
7. skanerów: 1 pkt.

”.

1. Dotyczy Załącznik nr 1 do SIWZ – Formularz oferty.

Prosimy o wyjaśnienie, czy w ramach kryteriów opisanych w punktach 6, 7 i 8 formularza ofertowego, Zamawiający dopuści aby wskazanie oferowanego rozwiązania zostało zrealizowane poprzez wykreślenie pozostałych (nie oferowanych) rozwiązań, a nie poprzez zakreślenie właściwej litery.

Zamawiający dopuszcza zastosowanie każdego innego sposobu oznaczenia wybranej opcji w sposób nie budzący wątpliwości co do wybranej przez Wykonawcę opcji, np. wykreślenie pozostałych.

PAKIET 3

1. Dotyczy: Załącznik numer 2 – SzOPZ, punkt 5 , wymaganie WP4.

Prosimy o wyjaśnienie, czy oprogramowanie do wirtualizacji również musi być w całości spolonizowane.

Zamawiający, dopuszcza nie w pełni spolonizowane oprogramowanie w zakresie: oprogramowania wbudowanego, np. firmware kart rozszerzeń, poleceń CLI, BIOS, UEFI, IDRAC, IPMI, iLO, itp.., oraz specjalistycznych narzędzi diagnostycznych i zarządzania dedykowanymi dla działów IT oraz narzędzi do wirtualizacji. W SIWZ znajduje sięzapis mówiący o tym: *„Wyjątek stanowią urządzenia wysoko specjalistyczne np. routery, przełączniki, serwery, macierze, punkty wifi, itp. dla których wymogiem minimalnym jest posiadanie interfejsów w języku minimum angielskim.”*

1. Dotyczy: Załącznik numer 2 – SzOPZ, punkt 6.1.8, wymaganie a)

Prosimy o doprecyzowanie czy zapis „(uwaga: po jednej konsoli dla każdej z lokalizacji terenowych)” oznacza, że dla każdej lokalizacji terenowej ma być również dostarczona osobna konsola zarządzająca o takich samych funkcjonalnościach jak dla całości środowiska, czy może zapis „jedna konsola do zarzadzania całym środowiskiem” oznacza możliwość zarządzania środowiskiem w całości razem z hostami zainstalowanymi w lokalizacjach terenowych.

Zapis oznacza, że do każdej z 12 lokalizacji ma zostać dostarczona oddzielna konsola do zarządzania lokalnym środowiskiem.

1. Dotyczy: Załącznik numer 2 – SzOPZ, punkt 6.1.8, wymaganie d)

Prosimy o wyjaśnienie, czy oprogramowanie do zarządzania maszynami wirtualnymi to element konsoli do zarządzania całym środowiskiem wirtualnym.

Intencją Zamawiającego było otrzymanie jednorodnego i spójnego narzędzia do zarządzania całą infrastrukturą w każdej z lokalizacji. Z uwagi na możliwość dostarczenia rozwiązań różnych producentów w różnych zakresach funkcjonalności, Zamawiający dopuszcza dostarczenie oddzielnego narzędzia do zarządzania daną funkcjonalnością [np. backup], wymaga jednak aby narzędzie miało możliwość pracy jako „przystawka” do nadrzędnego narzędzia zarządzania całą infrastrukturą.

1. Dotyczy: Załącznik numer 2 – SzOPZ, punkt 6.1.8, wymaganie e), f), g)

Prosimy o doprecyzowanie o co chodzi we wskazanych podpunktach. Opis wskazuje na oprogramowanie do backupu/archiwizacji.

Punkty te opisują jednorodne narzędzie do zarządzania infrastrukturą w różnych zakresach, między innymi w zakresie backupu, w którego zakresie znalazła się największa liczba zapisów.

1. Dotyczy: Załącznik nr 2 – SzOPZ, punkt 6.1.2 Wymagania minimalne dotyczące routera CE.

Zamawiający wymaga aby w każdym JST biorącym udział w projekcie zainstalowany został router CE. Prosimy o wyjaśnienie, jakie przesłanki kierowały Zamawiającym do wyspecyfikowania wymagań na routery CE. Zgodnie z zapisami w SIWZ routery CE mają służyć do podłączenia do wydzielonej sieci opartej o MPLS, co zdaniem Wykonawcy nie wymaga tak rozbudowanego routera jak wyspecyfikowany w SIWZ. Zamawiający wymaga by router miał jedynie 200Mb/s przepustowości.

Prosimy zatem o wyjaśnienie, do czego będzie potrzebna możliwość instalacji 6 modułów sieciowych z portami eth i SFP jeżeli będą one pracowały z ułamkiem swojej prędkości.
Czy Zamawiający chce wykorzystać router jako przełącznik? Jest to zdaniem Wykonawcy pozbawione sensu, ze względu na cenę modułu rozszerzeń a przede wszystkim bardzo niewielkiej wydajności całego routera (zwłaszcza, że jednocześnie Zamawiający wymaga dostawy szybkich przełączników sieciowych).

Prosimy o wyjaśnienie, do czego Zamawiający chce wykorzystać DSP. Do czego jest Zamawiającemu potrzebna możliwość instalacji modułu DSP o 128 kanałach?

Prosimy o wyjaśnienie, do czego Zamawiający chce wykorzystać możliwość instalacji
w routerze kart z portami FXS czy FX. Czy zamawiający planuje budowę sieci PSTN?

Prosimy o wyjaśnienie, do czego Zamawiający chce wykorzystać możliwość terminowania przez router CE aż 3000 kanałów IPSEC.

Wymaganie: Architektura - 3 Urządzenie musi posiadać zainstalowany, sprzętowy moduł akceleracji szyfrowania DES/3DES/AES.

Sprzętowy moduł akceleracji szyfracji dla tak niewielkiej przepustowości jaka jest wymaga
w SIWZ, jest w opinii Wykonawcy próbą ograniczenia konkurencji. Przy takich przepustowościach moduł taki nie jest stosowany (nie ma potrzeby stosowania) przez producentów routerów CE.

Wymaganie: Podstawowe wymaganie sprzętowe – 4.

Wymagania by port konsoli był wykonany w postaci portu USB noszą znamiona chęci ograniczenia konkurencji – port w postaci RJ45 nie wpływa w żaden negatywny sposób na funkcjonalność urządzenia.

Wykonawca odnosi wrażenie, iż wymagania stawiane przez Zamawiającego urządzeniu router CE są mocno przewymiarowane a co za tym idzie bardzo kosztowne. Jest to zdaniem Wykonawcy nieekonomiczne i może narazić Zamawiającego na zarzut niegospodarności
i niewłaściwego gospodarowania środkami publicznymi.

W związku z powyższym prosimy o potwierdzenie, że Zamawiający dopuści zaoferowanie jako router CE urządzenia, o parametrach nie gorszych niż niżej opisane, które to urządzenie zdaniem Wykonawcy będzie wystarczającym rozwiązaniem, uwzględniającym wszystkie realne potrzeby w ramach oferowanego systemu.

|  |  |
| --- | --- |
| Lp. | Parametry |
| 1 | System zabezpieczeń musi realizować zadania firewall, wykonując kontrolę na poziomie sieci oraz aplikacji |
| 2 | Urządzenie systemu zabezpieczeń musi posiadać możliwość uruchomienia modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS). Aktualizacja bazy sygnatur ataków (IPS) powinna odbywać się na żądanie bądź automatycznie zgodnie z ustalonym w konfiguracji harmonogramem.  |
| 3 | Urządzenie systemu zabezpieczeń musi posiadać możliwość uruchomienia modułu ochrony antywirusowej kontrolującego pocztę elektronicznej SMTP, POP3, IMAP, FTP oraz HTTP. Włączenie kontroli antywirusowej nie wymaga dodatkowego serwera. |
| 4 | Urządzenie systemu zabezpieczeń musi posiadać możliwość uruchomienia modułu kontroli antyspamowej działającego w oparciu o mechanizm blacklist. Włączenie kontroli antyspamowej nie wymaga dodatkowego serwera. |
| 5 | Urządzenie systemu zabezpieczeń musi posiadać możliwość uruchomienia modułu filtrowania stron WWW w zależności od kategorii treści stron. Włączenie filtrowania stron WWW nie wymaga dodatkowego serwera. Powyższe funkcjonalności (IPS, antywirus, antyspam, filtrowanie stron) mogą być dostępne po wykupieniu odpowiedniej licencji, która nie wchodzi w zakres niniejszego postępowania. |
| 6 | Urządzenie musi realizować zarządzanie pasmem sieci (QoS) oraz musi mieć możliwość zestawiania zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. |
| 7 | Urządzenie w obudowie 1U. Obudowa urządzenia musi być wykonana z metalu. Posiadać pasywne chłodzenie |
| 8 | Urządzenie zabezpieczeń musi być sterowane przez opracowany przez producenta zabezpieczeń dedykowany system operacyjny. |
| 9 | System zabezpieczeń musi być dostarczany jako dedykowane urządzenie sieciowe nie posiadające wrażliwych na awarie elementów sprzętowych (np. twardego dysku). |
| 10 | System zabezpieczeń nie może posiadać ograniczeń na liczbę chronionych komputerów w sieci wewnętrznej. |
| 11 | System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa). Polityki definiowane są pomiędzy dowolnymi strefami bezpieczeństwa. Urządzenie musi obsługiwać nie mniej niż 32 stref bezpieczeństwa. |
| 12 | Urządzenie zabezpieczeń musi posiadać przepływność nie mniej niż 3000 Mb/s (dla dużych pakietów) i nie mniej niż 1000 Mb/s dla ruchu dla ruchu IMIX; nie mniejszą niż 100 Mb/s dla IPSec VPN (SHA2/AES-256) i obsługiwać nie mniej niż 2000 polityk bezpieczeństwa. Urządzenie musi umożliwiać uruchomienie protokołów routingu IP/MPLS minimum: OSFP, IS-IS, BGP, LDP i RSVP oraz konfiguracji usług IP/MPLS minimum: L2VPN, L3VPN |
| 13 | Przepustowość systemu IPS musi być nie mniejsza niż 300 Mb/s |
| 15 | Urządzenie zabezpieczeń musi być wyposażone w 8 portów Gigabit Ethernet 10/100/1000 Base-T oraz 8 portów SFP.  |
| 17 | Urządzenie musi zapewniać obsługę 512 sieci VLAN |
| 18 | Sieci VPN tworzone przez system zabezpieczeń muszą działać poprawnie w środowiskach sieciowych, gdzie na drodze VPN wykonywana jest translacja adresów NAT. System zabezpieczeń musi posiadać zaimplementowany mechanizm IPSec NAT Traversal dla konfiguracji VPN client-to-site oraz site-to-site. |
| 19 | System zabezpieczeń musi posiadać zaimplementowane mechanizmy monitorowania stanu tuneli VPN i stałego utrzymywania ich aktywności (tzn. po wykryciu nieaktywności tunelu automatycznie następuje negocjacja IKE). |
| 20 | Konfiguracja VPN musi odbywać się w oparciu o reguły polityki bezpieczeństwa (Policy-based VPN) oraz ustawienia rutingu (Routing-based VPN). Co najmniej 1000 tuneli IPsec. |
| 21 | Urządzenie musi obsługiwać nie mniej niż 8 wirtualnych ruterów posiadających odrębne tabele rutingu, umożliwiające podłączenie do urządzenia sieci o tej samej adresacji IP. Urządzenie musi obsługiwać protokoły rutingu RIP, OSPF i BGP. |
| 22 | Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń. |
| 23 | Zarządzanie funkcjami zabezpieczeń w pełnym zakresie musi odbywać się z linii poleceń (CLI), graficznej konsoli GUI, oraz scentralizowanego systemu zarządzania. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). |
| 24 | System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Administratorzy mogą być uwierzytelniani za pomocą haseł statycznych oraz haseł dynamicznych (RADIUS). |
| 25 | System zabezpieczeń musi posiadać mechanizmy uwierzytelniania tożsamości użytkowników za pomocą haseł statycznych i dynamicznych. |
| 26 | System zabezpieczeń musi wykonywać statyczną i dynamiczną translację adresów NAT.  |
| 27 | System zabezpieczeń musi posiadać możliwość pracy w konfiguracji odpornej na awarie – HA (High Availability) |
| 28 | Urządzenie musi obsługiwać możliwość inspekcji podejrzanego ruchu/zawartości plików, co najmniej z rozszerzeniem \*.exe przy pomocy tzw. Sandboxingu realizowanego w usłudze chmurowej lub w postaci dedykowanego urządzenia. |
| 29 | Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim. |
| 30 | Zamawiający wymaga, aby dostarczone urządzenie posiadało gwarancję minimum 2 lata, świadczoną przez Wykonawcę na bazie wsparcia producenta. Wymiana uszkodzonego elementu w trybie min. 8x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu przekazania przedmiotu zamówienia. |

Zamawiający określił minimalne parametry routera w różnych zakresach w sposób w jaki realnie będzie wykorzystywany. Zarówno możliwość instalacji modułów jak i ich funkcjonalności wynikają z planowanych w przyszłości możliwych kierunkach rozwoju infrastruktury Zamawiającego. Zamawiajacy oczekuje możliwości rozbudowy w związku z planowanymi w niedalekiej przyszłości innymi projektami informatycznymi. Jednocześnie Zamawiający poprawił błędne zapisy w SIWZ dotyczące powyższego zakresu.

PAKIET 4

1. Dotyczy Załączniku nr 2 do SIWZ, pkt. 6.1.3      Wymagania minimalne dotyczące serwera AD – wariant I , Tabela 7 na str. 22 LP 1 - w minimalnych wymaganiach dotyczących serwera napisano: "Maksymalnie 2U RACK 19” (wraz z wszystkimi elementami niezbędnymi do zamontowania serwera w oferowanej szafie)."oraz pkt. 6.1.4      Wymagania minimalne dotyczące serwera AD – wariant II , Tabela 8 na str. 24 LP 1 gdzie w minimalnych wymaganiach dotyczących serwera napisano: "Maksymalnie 2U RACK 19” (wraz z wszystkimi elementami niezbędnymi do zamontowania serwera w oferowanej szafie)." Jednocześnie w pkt. 6.2.1      Informacje ogólne na str. 38 napisano: "Zamawiający zapewnia także zasilanie niezbędne do funkcjonowania urządzeń oraz miejsce w szafach Rack" oraz w Tabeli 17 kod: WSZL23 napisano: "Zamawiający wymaga minimalnej struktury PEL : 1 gniazdo RJ45 + 1 gniazdo 230V. Wszystkie gniazda RJ45 zakończone we wskazanych przez zamawiającego serwerowniach / szafach dystrybucyjnych RACK na patchpanelach kat min. 5E." Wykonawca  zauważa rozbieżności w przytoczonych zapisach w zakresie dostarczenia szaf RACK, w związku z powyższym prosimy o wyjaśnienie czy:

a) Wykonawca ma dostarczyć szafy RACK do lokalizacji Zamawiającego a jeśli tak to prosimy o podanie parametrów tych szaf (gabaryty, wymagane wyposażenie)?

b) Zamawiający zapewnia szafy RACK we własnym zakresie dla wszystkich lokalizacji natomiast Wykonawca ma doposażyć szafy RACK w patchpanele kat min. 5E?

Zamawiający zapewni szafy RACK i miejsce w tych szafach, do Wykonawcy należy dostarczeni i zainstalowanie patchpaneli i sprzętu aktywnego w tych szafach. Zamawiający jest przygotowany na objętość instalowanych urządzeń do 42U w każdej lokalizacji.

2. Zamawiający w Załączniku nr 2 do SIWZ w Tabeli nr 1 Wymagania minimalne dotyczące Routera CE stawia wymaganie aby dostarczone urządzenie posiadało gwarancję minimum 2 lata, świadczoną przez Wykonawcę na bazie wsparcia producenta. Wymiana uszkodzonego elementu w trybie min. 8x5xNBD.

- Prosimy o potwierdzenie, iż wskazany wymóg w zakresie długości trwania gwarancji (na okres min. 2 lat) musi być ściśle skorelowany z okresem na jaki dany Wykonawca deklaruje świadczenie usługi wsparcia dla całości systemu gdzie okres 2 lat jest najkrótszym z dopuszczalnych okresów co oznacza, iż w przypadku deklaracji o objęciu systemu gwarancją np. na okres 3 lat wspomniany router musi być objęty gwarancją świadczoną przez Wykonawcę na bazie wsparcia producenta na analogiczny okres tj. 3 lat, itd.

Zamawiający wymaga podania w Załączniku nr 1 do SIWZ – Formularzu oferty, okresu na jaki zostanie przedłużona gwarancja w zakresie:

1. serwerów: ………… miesięcy.
2. macierzy: ………… miesięcy
3. przełączników: ………… miesięcy.
4. routerów: ………… miesięcy.
5. komputerów: ………… miesięcy.
6. drukarek: ………… miesięcy.
7. skanerów: ………… miesięcy.

Jednocześnie Zamawiajacy nie wymaga potwierdzenia od Wykonawcy zawarcia umowy z Producentem na świadczenie usługi gwarancji / serwisu po minimalnym dwuletnim okresie gwarancyjnym, ciężar świadczenia usługi spoczywa wyłącznie na Wykonawcy, z którym Zamawiajacy podpisuje umowę.

1. Czy Zamawiający dla zweryfikowania stawianego wymogu w zakresie zapewnienia wsparcia producenta dla routera CE będzie wymagał od Wykonawcy okazania potwierdzenia ze strony producenta lub jego autoryzowanego partnera w Polsce o wykupieniu przez Wykonawcę dla urządzenia pakietu serwisowego na wymagany okres czasu umożliwiającego świadczenie usług gwarancji ?

Zamawiający podpisuje Umowę z Wykonawcą, i na Wykonawcy spoczywa obowiązek zabezpieczenia się w odpowiedni sposób na wypadek awarii. Zamawiający nie wymaga przedłożenia żadnych dokumentów potwierdzających objęcia wsparciem serwisowym urządzeń ze strony Producenta po minimalnym dwuletnim okresie gwarancyjnym. Zamawiający będzie domagał się dokumentów poswiadczających wsparcie serwisowe ze strony producenta w dwuletnim okresie minimalnym. W razie opóźnienia w usunięciu awarii na Wykonawcę będą nakładane kary zgodnie z Umową.

1. Zamawiający wymaga wymiany uszkodzonego elementu w trybie min. 8x5xNBD. Czy w kontekście tak brzmiącego wymagania dla routera CE i realizacji naprawy/wymiany urządzenia zgodnie z wymaganym reżimem Zamawiający uzna, iż spełniony jest wymóg w zakresie SLA w odniesieniu do definicji Dysfunkcji (załącznik nr 6) i jej kryteriów i górnych wymagań czasowych dla poszczególnych typów dysfunkcji (Procedura podejmowania Prac Serwisowych, pkt. 7, zał. nr 6) a jeśli tak to czy uszkodzenie wspomnianego urządzenia będzie klasyfikowane w kategorii Dysfunkcji jako „Awaria” ?

Każdorazowo przy występowaniu Dysfunkcji, Zamawiający określi jej kategorię. Również w zakresie Routera należy stosować się do Kategorii Dysfunkcji określonej w słowniku pojęć. Jeśli Router uniemożliwi pracę Jednostki [np. poprzez brak dostępu do systemów zainstalowanych w Jednostce Centralnej] należy sklasyfikować daną Dysfunkcję jako Krytyczną i postępować zgodnie z zapisami Umowy. Zapis „8x5” określa gotowość serwisu w trybie 8godzin przez 5 dni w tygodniu [czyli w Godzinach pracy Zamawiającego].

3. Zamawiający w Załączniku nr 2 do SIWZ w Tabeli nr 2 Wymagania minimalne dotyczące Serwera Active Directory - wariant I stawia wymaganie aby dostarczone urządzenie posiadało wsparcie serwisowe minimum 2 lata, w trybie min. 9h/5dni.

1. Prosimy o potwierdzenie, iż wskazany wymóg w zakresie długości trwania wsparcia serwisowego (na okres min. 2 lat) musi być ściśle skorelowany z okresem na jaki dany Wykonawca deklaruje świadczenie usługi wsparcia dla całości systemu gdzie okres 2 lat jest najkrótszym z dopuszczalnych okresów co oznacza, iż w przypadku deklaracji o objęciu systemu gwarancją np. na okres 3 lat wspomniany serwer musi być objęty wsparciem na analogiczny okres tj. 3 lat, itd.

Zamawiający wymaga podania w Załączniku nr 1 do SIWZ – Formularzu oferty, okresu na jaki zostanie przedłużona gwarancja w zakresie:

1. serwerów: ………… miesięcy.
2. macierzy: ………… miesięcy
3. przełączników: ………… miesięcy.
4. routerów: ………… miesięcy.
5. komputerów: ………… miesięcy.
6. drukarek: ………… miesięcy.
7. skanerów: ………… miesięcy.

Jednocześnie Zamawiajacy nie wymaga potwierdzenia od Wykonawcy zawarcia umowy z Producentem na świaedczenie ugługi gwarancji / serwisu po minimalnym dwuletnim okresie gwarancyjnym, ciężar świadczenia usługi spoczywa wyłącznie na Wykonawcy, z którym Zamawiajacy podpisuje umowę.

1. Czy Zamawiający dla zweryfikowania stawianego wymogu w zakresie zapewnienia wsparcia dla w/w serwera będzie wymagał od Wykonawcy okazania potwierdzenia ze strony producenta lub jego autoryzowanego partnera w Polsce o wykupieniu przez Wykonawcę dla urządzenia pakietu serwisowego na wymagany okres czasu umożliwiającego świadczenie usług wsparcia ?

Zamawiający podpisuje Umowę z Wykonawcą, i na Wykonawcy spoczywa obowiązek zabezpieczenia się w odpowiedni sposób na wypadek awarii. Zamawiający nie wymaga przedłożenia żadnych dokumentów potwierdzających objęcia wsparciem serwisowym urządzeń ze strony Wykonawcy po minimalnym dwuletnim okresie gwarancyjnym. Zamawiający będzie domagał się dokumentów poswiadczających wsparcie serwisowe ze strony producenta w dwuletnim okresie minimalnym. W razie opóźnienia w usunięciu awarii na Wykonawcę będą nakładane kary zgodnie z Umową.

1. Zamawiający wymaga realizacji wsparcia w trybie min. 9h x 5dni. Czy w kontekście tak brzmiącego wymagania dla w/w serwera i realizacji naprawy/wymiany urządzenia zgodnie z wymaganym reżimem Zamawiający uzna, iż spełniony jest wymóg w zakresie SLA w odniesieniu do definicji Dysfunkcji (załącznik nr 6) i jej Kryteriów i górnych wymagań czasowych dla poszczególnych typów dysfunkcji (Procedura podejmowania Prac Serwisowych, pkt. 7, zał. nr 6) a jeśli tak to czy uszkodzenie wspomnianego urządzenia będzie klasyfikowane w kategorii Dysfunkcji jako „Awaria” ?

Każdorazowo przy występowaniu Dysfunkcji, Zamawiający określi jej kategorię. Również w zakresie Routera należy stosować się do Kategorii Dysfunkcji określonej w słowniku pojęć. Jeśli Router uniemożliwi pracę Jednostki [np. poprzez brak dostępu do systemów zainstalowanych w Jednostce Centralnej] należy sklasyfikować daną Dysfunkcję jako Krytyczną i postępować zgodnie z zapisami Umowy. Zapis „8x5” określa gotowość serwisu w trybie 8godzin przez 5 dni w tygodniu [czyli w Godzinach pracy Zamawiającego].

4. Zamawiający w Załączniku nr 2 do SIWZ w Tabeli nr 8 Wymagania minimalne dotyczące Serwera Active Directory - wariant II stawia wymaganie aby dostarczone urządzenie posiadało wsparcie serwisowe minimum 2 lata, w trybie min. 9h/5dni.

1. Prosimy o potwierdzenie, iż wskazany wymóg w zakresie długości trwania wsparcia serwisowego (na okres min. 2 lat) musi być ściśle skorelowany z okresem na jaki dany Wykonawca deklaruje świadczenie usługi wsparcia dla całości systemu gdzie okres 2 lat jest najkrótszym z dopuszczalnych okresów co oznacza, iż w przypadku deklaracji o objęciu systemu gwarancją np. na okres 3 lat wspomniany serwer musi być objęty wsparciem na analogiczny okres tj. 3 lat, itd.
2. Czy Zamawiający dla zweryfikowania stawianego wymogu w zakresie zapewnienia wsparcia dla w/w serwera będzie wymagał od Wykonawcy okazania potwierdzenia ze strony producenta lub jego autoryzowanego partnera w Polsce o wykupieniu przez Wykonawcę dla urządzenia pakietu serwisowego na wymagany okres czasu umożliwiającego świadczenie usług wsparcia ?

Zamawiający podpisuje Umowę z Wykonawcą, i na Wykonawcy spoczywa obowiązek zabezpieczenia się w odpowiedni sposób na wypadek awarii. Zamawiający nie wymaga przedłożenia żadnych dokumentów potwierdzających objęcia wsparciem serwisowym urządzeń ze strony Wykonawcy po minimalnym dwuletnim okresie gwarancyjnym. Zamawiający będzie domagał się dokumentów poswiadczających wsparcie serwisowe ze strony producenta w dwuletnim okresie minimalnym. W razie opóźnienia w usunięciu awarii na Wykonawcę będą nakładane kary zgodnie z Umową.

1. Zamawiający wymaga realizacji wsparcia w trybie min. 9h x 5dni. Czy w kontekście tak brzmiącego wymagania dla w/w serwera i realizacji naprawy/wymiany urządzenia zgodnie z wymaganym reżimem Zamawiający uzna, iż spełniony jest wymóg w zakresie SLA w odniesieniu do definicji Dysfunkcji (załącznik nr 6) i jej Kryteriów i górnych wymagań czasowych dla poszczególnych typów dysfunkcji (Procedura podejmowania Prac Serwisowych, pkt. 7, zał. nr 6) a jeśli tak to czy uszkodzenie wspomnianego urządzenia będzie klasyfikowane w kategorii Dysfunkcji jako „Awaria” ?

Każdorazowo przy występowaniu Dysfunkcji, Zamawiający określi jej kategorię. Również w zakresie Serwera należy stosować się do Kategorii Dysfunkcji określonej w słowniku pojęć. Jeśli Serwer uniemożliwi pracę Jednostki [np. poprzez brak dostępu do systemów] należy sklasyfikować daną Dysfunkcję jako Krytyczną i postępować zgodnie z zapisami Umowy. Zapis „9x5” określa gotowość serwisu w trybie 9 godzin przez 5 dni w tygodniu [w Godzinach pracy Zamawiającego].

5. Zamawiający w Załączniku nr 2 do SIWZ w Tabeli nr 9 Wymagania minimalne dotyczące macierzy dyskowej w zasobach lokalnych stawia wymaganie aby dostarczone urządzenie posiadało wsparcie serwisowe minimum 2 lata, w trybie min. 9h/5dni.

1. Prosimy o potwierdzenie, iż wskazany wymóg w zakresie długości trwania wsparcia serwisowego (na okres min. 2 lat) musi być ściśle skorelowany z okresem na jaki dany Wykonawca deklaruje świadczenie usługi wsparcia dla całości systemu gdzie okres 2 lat jest najkrótszym z dopuszczalnych okresów co oznacza, iż w przypadku deklaracji o objęciu systemu gwarancją np. na okres 3 lat wspomniana macierz musi być objęta wsparciem na analogiczny okres tj. 3 lat, itd.

Zamawiający wymaga podania w Załączniku nr 1 do SIWZ – Formularzu oferty, okresu na jaki zostanie przedłużona gwarancja w zakresie:

1. serwerów: ………… miesięcy.
2. macierzy: ………… miesięcy
3. przełączników: ………… miesięcy.
4. routerów: ………… miesięcy.
5. komputerów: ………… miesięcy.
6. drukarek: ………… miesięcy.
7. skanerów: ………… miesięcy.

Jednocześnie Zamawiajacy nie wymaga potwierdzenia od Wykonawcy zawarcia umowy z Producentem na świaedczenie ugługi gwarancji / serwisu w tym okresie, ciężar świadczenia usługi spoczywa wyłącznie na Wykonawcy, z którym Zamawiajacy podpisuje umowę.

1. Czy Zamawiający dla zweryfikowania stawianego wymogu w zakresie zapewnienia wsparcia dla w/w macierzy będzie wymagał od Wykonawcy okazania potwierdzenia ze strony producenta lub jego autoryzowanego partnera w Polsce o wykupieniu przez Wykonawcę dla urządzenia pakietu serwisowego na wymagany okres czasu umożliwiającego świadczenie usług wsparcia ?

Zamawiający podpisuje Umowę z Wykonawcą, i na Wykonawcy spoczywa obowiązek zabezpieczenia się w odpowiedni sposób na wypadek awarii. Zamawiający nie wymaga przedłożenia żadnych dokumentów potwierdzających objęcia wsparciem serwisowym urządzeń ze strony Wykonawcy po minimalnym dwuletnim okresie gwarancyjnym. Zamawiający będzie domagał się dokumentów poswiadczających wsparcie serwisowe ze strony producenta w dwuletnim okresie minimalnym. W razie opóźnienia w usunięciu awarii na Wykonawcę będą nakładane kary zgodnie z Umową.

1. Zamawiający wymaga realizacji wsparcia w trybie min. 9h x 5dni. Czy w kontekście tak brzmiącego wymagania dla w/w macierzy i realizacji naprawy/wymiany urządzenia zgodnie z wymaganym reżimem Zamawiający uzna, iż spełniony jest wymóg w zakresie SLA w odniesieniu do definicji Dysfunkcji (załącznik nr 6) i jej Kryteriów i górnych wymagań czasowych dla poszczególnych typów dysfunkcji (Procedura podejmowania Prac Serwisowych, pkt. 7, zał. nr 6) a jeśli tak to czy uszkodzenie wspomnianego urządzenia będzie klasyfikowane w kategorii Dysfunkcji jako „Awaria” ?

Każdorazowo przy występowaniu Dysfunkcji, Zamawiający określi jej kategorię. Również w zakresie Macierzy należy stosować się do Kategorii Dysfunkcji określonej w słowniku pojęć. Jeśli Macierz uniemożliwi pracę Jednostki [np. poprzez brak dostępu do systemów] należy sklasyfikować daną Dysfunkcję jako Krytyczną i postępować zgodnie z zapisami Umowy. Zapis „9x5” określa gotowość serwisu w trybie 9 godzin przez 5 dni w tygodniu [w Godzinach pracy Zamawiającego].

6. Zamawiający w Załączniku nr 2 do SIWZ w Tabeli nr 10 Wymagania minimalne dotyczące komputera stacjonarnego z monitorem stawia wymaganie aby dostarczone urządzenie posiadało wsparcie serwisowe minimum 2 lata, w trybie min. 9h/5dni.

1. Prosimy o potwierdzenie bądź zaprzeczenie, iż wskazany wymóg w zakresie długości trwania wsparcia serwisowego (na okres min. 2 lat) musi być ściśle skorelowany z okresem na jaki dany Wykonawca deklaruje świadczenie usługi wsparcia dla całości systemu gdzie okres 2 lat jest najkrótszym z dopuszczalnych okresów co oznacza, iż w przypadku deklaracji o objęciu systemu gwarancją np. na okres 3 lat wspomniany komputer musi być objęty wsparciem na analogiczny okres tj. 3 lat, itd.

Zamawiający wymaga podania w Załączniku nr 1 do SIWZ – Formularzu oferty, okresu na jaki zostanie przedłużona gwarancja w zakresie:

1. serwerów: ………… miesięcy.
2. macierzy: ………… miesięcy
3. przełączników: ………… miesięcy.
4. routerów: ………… miesięcy.
5. komputerów: ………… miesięcy.
6. drukarek: ………… miesięcy.
7. skanerów: ………… miesięcy.

Jednocześnie Zamawiajacy nie wymaga potwierdzenia od Wykonawcy zawarcia umowy z Producentem na świaedczenie ugługi gwarancji / serwisu w tym okresie, ciężar świadczenia usługi spoczywa wyłącznie na Wykonawcy, z którym Zamawiajacy podpisuje umowę.

1. Czy Zamawiający dla zweryfikowania stawianego wymogu w zakresie zapewnienia wsparcia dla w/w urządzenia będzie wymagał od Wykonawcy okazania potwierdzenia ze strony producenta lub jego autoryzowanego partnera w Polsce o wykupieniu przez Wykonawcę dla urządzenia pakietu serwisowego na wymagany okres czasu umożliwiającego świadczenie usług wsparcia ?

Zamawiający podpisuje Umowę z Wykonawcą, i na Wykonawcy spoczywa obowiązek zabezpieczenia się w odpowiedni sposób na wypadek awarii. Zamawiający nie wymaga przedłożenia żadnych dokumentów potwierdzających objęcia wsparciem serwisowym urządzeń ze strony Wykonawcy. W razie opóźnienia w usunięciu awarii na Wykonawcę będą nakładane kary zgodnie z Umową.

1. Zamawiający wymaga realizacji wsparcia w trybie min. 9h x 5dni. Czy w kontekście tak brzmiącego wymagania dla w/w urządzenia i realizacji naprawy/wymiany urządzenia zgodnie z wymaganym reżimem Zamawiający uzna, iż spełniony jest wymóg w zakresie SLA w odniesieniu do definicji Dysfunkcji (załącznik nr 6) i jej Kryteriów i górnych wymagań czasowych dla poszczególnych typów dysfunkcji (Procedura podejmowania Prac Serwisowych, pkt. 7, zał. nr 6) a jeśli tak to czy uszkodzenie wspomnianego urządzenia będzie klasyfikowane w kategorii Dysfunkcji jako „Awaria” ?

Skanery, drukarki, punkty wifi i komputery nie stanowią elementów krytycznych z punktu widzenia pracy Systemu, dlatego ich Dysfunkcje nie będą klasyfikowane jako Krytyczne ani Awarie. W skrajnych przypadkach, np. kiedy Dysfunkcji ulegnie większa liczba urządzań jednocześnie, kolejne Dysfunkcje mogą być zgłaszane jako awarie, z powodu „wyczerpującego” się sprzętu na którym możliwa jest praca pracowników Zamawiającego.

7. Zamawiający w Załączniku nr 2 do SIWZ w Tabeli nr 11 Wymagania minimalne dotyczące komputera przenośnego typu laptop stawia wymaganie aby dostarczone urządzenie posiadało wsparcie serwisowe minimum 2 lata, w trybie min. 9h/5dni.

1. Prosimy o potwierdzenie bądź zaprzeczenie, iż wskazany wymóg w zakresie długości trwania wsparcia serwisowego (na okres min. 2 lat) musi być ściśle skorelowany z okresem na jaki dany Wykonawca deklaruje świadczenie usługi wsparcia dla całości systemu gdzie okres 2 lat jest najkrótszym z dopuszczalnych okresów co oznacza, iż w przypadku deklaracji o objęciu systemu gwarancją np. na okres 3 lat wspomniany komputer musi być objęty wsparciem na analogiczny okres tj. 3 lat, itd.

Zamawiający wymaga podania w Załączniku nr 1 do SIWZ – Formularzu oferty, okresu na jaki zostanie przedłużona gwarancja w zakresie:

1. serwerów: ………… miesięcy.
2. macierzy: ………… miesięcy
3. przełączników: ………… miesięcy.
4. routerów: ………… miesięcy.
5. komputerów: ………… miesięcy.
6. drukarek: ………… miesięcy.
7. skanerów: ………… miesięcy.

Jednocześnie Zamawiajacy nie wymaga potwierdzenia od Wykonawcy zawarcia umowy z Producentem na świaedczenie ugługi gwarancji / serwisu w tym okresie, ciężar świadczenia usługi spoczywa wyłącznie na Wykonawcy, z którym Zamawiajacy podpisuje umowę.

1. Czy Zamawiający dla zweryfikowania stawianego wymogu w zakresie zapewnienia wsparcia dla w/w urządzenia będzie wymagał od Wykonawcy okazania potwierdzenia ze strony producenta lub jego autoryzowanego partnera w Polsce o wykupieniu przez Wykonawcę dla urządzenia pakietu serwisowego na wymagany okres czasu umożliwiającego świadczenie usług wsparcia ?

Zamawiający podpisuje Umowę z Wykonawcą, i na Wykonawcy spoczywa obowiązek zabezpieczenia się w odpowiedni sposób na wypadek awarii. Zamawiający nie wymaga przedłożenia żadnych dokumentów potwierdzających objęcia wsparciem serwisowym urządzeń ze strony Wykonawcy. W razie opóźnienia w usunięciu awarii na Wykonawcę będą nakładane kary zgodnie z Umową.

1. Zamawiający wymaga realizacji wsparcia w trybie min. 9h x 5dni. Czy w kontekście tak brzmiącego wymagania dla w/w urządzenia i realizacji naprawy/wymiany urządzenia zgodnie z wymaganym reżimem Zamawiający uzna, iż spełniony jest wymóg w zakresie SLA w odniesieniu do definicji Dysfunkcji (załącznik nr 6) i jej Kryteriów i górnych wymagań czasowych dla poszczególnych typów dysfunkcji (Procedura podejmowania Prac Serwisowych, pkt. 7, zał. nr 6) a jeśli tak to czy uszkodzenie wspomnianego urządzenia będzie klasyfikowane w kategorii Dysfunkcji jako „Awaria” ?

Skanery, drukarki, punkty wifi i komputery nie stanowią elementów krytycznych z punktu widzenia pracy Systemu, dlatego ich Dysfunkcje nie będą klasyfikowane jako Krytyczne ani Awarie. W skrajnych przypadkach, np. kiedy Dysfunkcji ulegnie większa liczba urządzań jednocześnie, kolejne Dysfunkcje mogą być zgłaszane jako awarie, z powodu „wyczerpującego” się sprzętu na którym możliwa jest praca pracowników Zamawiającego.

8. Zamawiający w Załączniku nr 2 do SIWZ w Tabelach: nr 12 Wymagania minimalne dotyczące parametrów skanera małego, nr 13 Wymagania minimalne dotyczące parametrów skanera dużego , nr 14 Wymagania minimalne dotyczące parametrów drukarki etykiet stawia wymaganie aby dostarczone urządzenia posiadały wsparcie serwisowe minimum 2 lata, bez deklarowanego SLA.

1. Prosimy o potwierdzenie bądź zaprzeczenie, iż wskazany wymóg w zakresie długości trwania wsparcia serwisowego (na okres min. 2 lat) musi być ściśle skorelowany z okresem na jaki dany Wykonawca deklaruje świadczenie usługi wsparcia dla całości systemu gdzie okres 2 lat jest najkrótszym z dopuszczalnych okresów co oznacza, iż w przypadku deklaracji o objęciu systemu gwarancją np. na okres 3 lat wspomniane urządzenia muszą być objęte wsparciem na analogiczny okres tj. 3 lat, itd.

Zamawiający wymaga podania w Załączniku nr 1 do SIWZ – Formularzu oferty, okresu na jaki zostanie przedłużona gwarancja w zakresie:

1. serwerów: ………… miesięcy.
2. macierzy: ………… miesięcy
3. przełączników: ………… miesięcy.
4. routerów: ………… miesięcy.
5. komputerów: ………… miesięcy.
6. drukarek: ………… miesięcy.
7. skanerów: ………… miesięcy.

Jednocześnie Zamawiajacy nie wymaga potwierdzenia od Wykonawcy zawarcia umowy z Producentem na świaedczenie ugługi gwarancji / serwisu w tym okresie, ciężar świadczenia usługi spoczywa wyłącznie na Wykonawcy, z którym Zamawiajacy podpisuje umowę.

1. Czy Zamawiający dla zweryfikowania stawianego wymogu w zakresie zapewnienia wsparcia dla w/w urządzeń będzie wymagał od Wykonawcy okazania potwierdzenia ze strony producentów lub ich autoryzowanych partnerów w Polsce o wykupieniu przez Wykonawcę dla urządzeń pakietów serwisowych na wymagany okres czasu umożliwiających świadczenie usług wsparcia ?

Zamawiający podpisuje Umowę z Wykonawcą, i na Wykonawcy spoczywa obowiązek zabezpieczenia się w odpowiedni sposób na wypadek awarii. Zamawiający nie wymaga przedłożenia żadnych dokumentów potwierdzających objęcia wsparciem serwisowym urządzeń ze strony Wykonawcy. W razie opóźnienia w usunięciu awarii na Wykonawcę będą nakładane kary zgodnie z Umową.

1. Zamawiający nie definiuje parametrów wsparcia/SLA dla w/w urządzeń. Czy w kontekście braku wymagań na SLA dla w/w urządzeń i w odniesieniu do definicji Dysfunkcji (załącznik nr 6) i jej Kryteriów i górnych wymagań czasowych dla poszczególnych typów dysfunkcji (Procedura podejmowania Prac Serwisowych, pkt. 7, zał. nr 6) prosimy o określenie jak będzie klasyfikowana awaria w/w urządzeń (Błąd, Awaria, inaczej) ?

Skanery, drukarki, punkty wifi i komputery nie stanowią elementów krytycznych z punktu widzenia pracy Systemu, dlatego ich Dysfunkcje nie będą klasyfikowane jako Krytyczne ani Awarie. W skrajnych przypadkach, np. kiedy Dysfunkcji ulegnie większa liczba urządzań jednocześnie, kolejne Dysfunkcje mogą być zgłaszane jako awarie, z powodu „wyczerpującego” się sprzętu na którym możliwa jest praca pracowników Zamawiającego.

9. Zamawiający w Załączniku nr 2 do SIWZ w Tabeli nr 15 Wymagania minimalne dotyczące przełączników sieciowych stawia wymóg aby dostarczone urządzenie posiadało gwarancję minimum 2 lata, świadczoną przez Wykonawcę na bazie wsparcia producenta z SLA odpowiadającym dla Projektu.

1. Prosimy o potwierdzenie, iż wskazany wymóg w zakresie długości trwania gwarancji (na okres min. 2 lat) musi być ściśle skorelowany z okresem na jaki dany Wykonawca deklaruje świadczenie usługi wsparcia dla całości systemu gdzie okres 2 lat jest najkrótszym z dopuszczalnych okresów co oznacza, iż w przypadku deklaracji o objęciu systemu gwarancją np. na okres 3 lat wspomniany przełącznik musi być objęty gwarancją świadczoną przez Wykonawcę na bazie wsparcia producenta na analogiczny okres tj. 3 lat, itd.

Zamawiający wymaga podania w Załączniku nr 1 do SIWZ – Formularzu oferty, okresu na jaki zostanie przedłużona gwarancja w zakresie:

1. serwerów: ………… miesięcy.
2. macierzy: ………… miesięcy
3. przełączników: ………… miesięcy.
4. routerów: ………… miesięcy.
5. komputerów: ………… miesięcy.
6. drukarek: ………… miesięcy.
7. skanerów: ………… miesięcy.

Jednocześnie Zamawiajacy nie wymaga potwierdzenia od Wykonawcy zawarcia umowy z Producentem na świaedczenie ugługi gwarancji / serwisu w tym okresie, ciężar świadczenia usługi spoczywa wyłącznie na Wykonawcy, z którym Zamawiajacy podpisuje umowę.

1. Czy Zamawiający dla zweryfikowania stawianego wymogu w zakresie zapewnienia wsparcia producenta dla przełącznika będzie wymagał od Wykonawcy okazania potwierdzenia ze strony producenta lub jego autoryzowanego partnera w Polsce o wykupieniu przez Wykonawcę dla urządzenia pakietu serwisowego na wymagany okres czasu umożliwiającego świadczenie usług gwarancji ?

Zamawiający podpisuje Umowę z Wykonawcą, i na Wykonawcy spoczywa obowiązek zabezpieczenia się w odpowiedni sposób na wypadek awarii. Zamawiający nie wymaga przedłożenia żadnych dokumentów potwierdzających objęcia wsparciem serwisowym urządzeń ze strony Wykonawcy po dwuletnim okresie minimalnym gwarancji. Zamawiający będzie domagał się dokumentów poswiadczających wsparcie serwisowe ze strony producenta w dwuletnim okresie minimalnym. W razie opóźnienia w usunięciu awarii na Wykonawcę będą nakładane kary zgodnie z Umową.

1. Zamawiający wymaga wymiany uszkodzonego elementu zgodnie z SLA Projektu. W kontekście definicji Dysfunkcji (załącznik nr 6) i jej Kryteriów i górnych wymagań czasowych dla poszczególnych typów dysfunkcji (Procedura podejmowania Prac Serwisowych, pkt. 7, zał. nr 6) prosimy o wyjaśnienie jak będzie klasyfikowane uszkodzenie skutkujące wyłączeniem z eksploatacji przełącznika (jako Awaria, Błąd, inaczej) ?

Przeczniki stanowią elementy krytyczne z punktu widzenia pracy Systemu, dlatego ich Dysfunkcje będą klasyfikowane jako Krytyczne lub Awarie.

10. Zamawiający w Załączniku nr 2 do SIWZ w Tabeli nr 19 Wymagania minimalne dotyczące parametrów punktów WiFi stawia wymóg aby dostarczone urządzenie posiadało gwarancję minimum 2 lata, świadczoną przez Wykonawcę na bazie wsparcia producenta z SLA odpowiadającym dla Projektu.

1. Prosimy o potwierdzenie, iż wskazany wymóg w zakresie długości trwania gwarancji (na okres min. 2 lat) musi być ściśle skorelowany z okresem na jaki dany Wykonawca deklaruje świadczenie usługi wsparcia dla całości systemu gdzie okres 2 lat jest najkrótszym z dopuszczalnych okresów co oznacza, iż w przypadku deklaracji o objęciu systemu gwarancją np. na okres 3 lat wspomniany punkt dostępowy WiFi musi być objęty gwarancją świadczoną przez Wykonawcę na bazie wsparcia producenta na analogiczny okres tj. 3 lat, itd.

Zamawiający wymaga podania w Załączniku nr 1 do SIWZ – Formularzu oferty, okresu na jaki zostanie przedłużona gwarancja w zakresie:

1. serwerów: ………… miesięcy.
2. macierzy: ………… miesięcy
3. przełączników: ………… miesięcy.
4. routerów: ………… miesięcy.
5. komputerów: ………… miesięcy.
6. drukarek: ………… miesięcy.
7. skanerów: ………… miesięcy.

Jednocześnie Zamawiajacy nie wymaga potwierdzenia od Wykonawcy zawarcia umowy z Producentem na świaedczenie ugługi gwarancji / serwisu w tym okresie, ciężar świadczenia usługi spoczywa wyłącznie na Wykonawcy, z którym Zamawiajacy podpisuje umowę.

W pozostałych zakresach obowiązują zapisy wymienione w tabelach.

1. Czy Zamawiający dla zweryfikowania stawianego wymogu w zakresie zapewnienia wsparcia producenta dla przełącznika będzie wymagał od Wykonawcy okazania potwierdzenia ze strony producenta lub jego autoryzowanego partnera w Polsce o wykupieniu przez Wykonawcę dla urządzenia pakietu serwisowego na wymagany okres czasu umożliwiającego świadczenie usług gwarancji ?

Zamawiający podpisuje Umowę z Wykonawcą, i na Wykonawcy spoczywa obowiązek zabezpieczenia się w odpowiedni sposób na wypadek awarii. Zamawiający nie wymaga przedłożenia żadnych dokumentów potwierdzających objęcia wsparciem serwisowym urządzeń ze strony Wykonawcy. W razie opóźnienia w usunięciu awarii na Wykonawcę będą nakładane kary zgodnie z Umową.

1. Zamawiający wymaga wymiany uszkodzonego elementu zgodnie z SLA Projektu. W kontekście definicji Dysfunkcji (załącznik nr 6) i jej Kryteriów i górnych wymagań czasowych dla poszczególnych typów dysfunkcji (Procedura podejmowania Prac Serwisowych, pkt. 7, zał. nr 6) prosimy o wyjaśnienie jak będzie klasyfikowane uszkodzenie skutkujące wyłączeniem z eksploatacji punktu dostępowego WiFi (jako Awaria, Błąd, inaczej) ?

Punkty wifi nie stanowią elementów krytycznych z punktu widzenia pracy Systemu, dlatego ich Dysfunkcje nie będą klasyfikowane jako Krytyczne ani Awarie. W skrajnych przypadkach, np. kiedy Dysfunkcji ulegnie większa liczba urządzań jednocześnie, kolejne Dysfunkcje mogą być zgłaszane jako awarie, z powodu „wyczerpującego” się sprzętu na którym możliwe jest świadczenie usługi.

11. W Załączniku nr 2 do SIWZ, punkt 9.6 Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy, cześć WD13 Bezpieczeństwo i ochrona przed atakami, Zamawiający wymaga od Wykonawcy aby świadczył aktywny monitoring usług bezpieczeństwa zasobów IT Zamawiającego i reagował na ataki z wykorzystaniem specjalizowanego zespołu Security Operations Center (SOC), jednocześnie Zamawiający przedstawił swoje wymagania względem zespołu Security Operations Center (SOC) jedynie w odniesieniu do punktu I. tj. Ochrona przed atakami.

Prosimy o potwierdzenie, że monitoringiem i obsługą incydentów związanych z atakami ma zajmować się zespół Security Operations Center (SOC) jedynie w odniesieniu do usługi ochrony przed atakami wolumetrycznymi jak i atakami aplikacyjnymi typu DoS opisanej w pkt. I Ochrona przed atakami.

Zamawiający potwierdza że monitoringiem i obsługą incydentów związanych z atakami ma zajmować się zespół Security Operations Center (SOC) jedynie w odniesieniu do usługi ochrony przed atakami wolumetrycznymi jak i atakami aplikacyjnymi typu DoS opisanej w pkt. I Ochrona przed atakami.

12. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.1 Informacje ogólne – Zamawiający stawia wymaganie w brzmieniu: „Wszystkie punkty dostępowe zostaną rozmieszczone na terenie oraz wokół poszczególnych budynków urzędów administracji samorządowej biorącej udział w projekcie oraz wybranych lokalizacjach na terenie miejscowości” . Jednocześnie z opisu urządzeń zawartego w pkt. 6.3.3 „Wymagania minimalne punktów dostępowych” wynika, iż urządzenia są urządzeniami klasy „out-door” tj. przeznaczonymi do instalacji na otwartej przestrzeni i wystawionymi na działania czynników atmosferycznych.

Prosimy o potwierdzenie, iż wszystkie urządzenia realizujące funkcjonalność punktów dostępowych mają być urządzeniami typu „outdoor” i mają być instalowane poza wnętrzem budynków użyteczności publicznej bądź mieszkalnej (na fasadach lub dachach budynków, masztach, etc.)

Zamawiający wymaga dostarczenia 12 szt. AP w obudowach outdoor i 78 w obudowach indoor.

13. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wymaga od Wykonawcy aby świadczył aktywny monitoring usług bezpieczeństwa zasobów IT Zamawiającego i reagował na ataki z wykorzystaniem specjalizowanego zespołu Security Operations Center (SOC), jednocześnie Zamawiający przedstawił swoje wymagania względem zespołu Security Operations Center (SOC) jedynie w odniesieniu do punktu I. tj. „Ochrona przed atakami”. Prosimy o potwierdzenie, że monitoringiem i obsługą incydentów związanych z atakami ma zajmować się zespół Security Operations Center (SOC) jedynie w odniesieniu do usługi ochrony przed atakami wolumetrycznymi jak i atakami aplikacyjnymi typu DoS opisanej w pkt. I „Ochrona przed atakami”.

Zamawiający potwierdza że monitoringiem i obsługą incydentów związanych z atakami ma zajmować się zespół Security Operations Center (SOC) jedynie w odniesieniu do usługi ochrony przed atakami wolumetrycznymi jak i atakami aplikacyjnymi typu DoS opisanej w pkt. I Ochrona przed atakami.

14. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wskazał wymagania w zakresie usługi Cloud Firewall polegających na udostępnieniu przez Wykonawcę centralnego systemu logowania i raportowania. Zwracamy uwagę, że w specyfikacji brak jest wymagań technicznych parametryzujących ilość gromadzonych GB logów dziennie. Jest to bardzo istotny parametr w kontekście parametru wydajności a co za tym idzie zdolności do gromadzenia, przetwarzania i późniejszego raportowania przez system określonego wolumenu logów. Czy Zamawiający zaakceptuje centralny system logowania i raportowania umożliwiające gromadzenie logów na poziomie nie mniej niż 10 GB logów na dzień.

Z przyczyn oczywistych Zamawiający nie znając dostarczanego Systemu nie jest w stanie określić ilości logów generowanych przez dostarczane przez Wykonawcę urządzenia i usługi. Na Wykonawcy ciąży obowiązek zapewnienia dostępności logów przez okres minimum 30 dni. Zamawiający wymaga jednak aby każdorazowo przed wykasowaniem logów z systemu możliwa była ich archiwizacja na nośnikach zewnętrznych w celu późniejszej analizy – archiwizacja w zakresie Zamawiajacego.

15. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wskazał wymagania w zakresie usługi VI „System ochrony serwerów w JST”, której wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami IPS, AC, AV musi obsługiwać minimum 1500 Mbps. Czy Zamawiający uzna za spełniające wymagania rozwiązanie którego wydajność Kontroli Aplikacji (AC) jest na poziomie nie mniej niż 1500 Mbps i jednocześnie wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami IPS, AC, AV byłaby na poziomie nie mniej niż 400 Mbps.

Zamawiający zaakceptuje powyższe rozwiązanie.

16. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wskazał wymagania w zakresie usługi Antymalware. Czy Zamawiający wymaga od Wykonawcy aby posiadał na terenie Polski system bezpieczeństwa Sandbox zbudowany w architekturze wysoko dostępnej (HA)?

Zamawiający nie wymaga posiadania na terenie Polski systemu Sandbox zbudowanego w architekturze HA.

17. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wskazał wymagania w zakresie usługi Antymalware. Czy Zamawiający wymaga od Wykonawcy, aby usługa Antymalware celem zwiększenia poziomu bezpieczeństwa była zintegrowana z usługami „Cloud Firewall” , „Secure Cloud Mail Gateway” i „System ochrony serwerów w JST”?

Zamawiający wymaga aby usługa Animalware była zintegrowana z usługami Clodud Firewall, Secure Cloud Mail Gateway oraz systemem ochrony serwerów w JST.

18. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wskazał wymagania w zakresie usługi Antymalware. Zwracamy uwagę, że w wymaganiach brak jest informacji odnośnie wymaganych systemów operacyjnych uruchamianych na maszynach VM jakie mają być emulowane w systemie bezpieczeństwa Sandbox. Czy Zamawiający potwierdza, że system bezpieczeństwa Sandbox, musi wspierać systemy operacyjne Microsoft Windows 7, Microsoft Windows 8.1, Microsoft Windows 10, pakiety biurowe Microsoft Office 2007, Microsoft Office 2010, Microsoft Office 2013 oraz umożliwiać wgranie dostosowanego do faktycznych potrzeb Zamawiającego obrazu systemu operacyjnego Microsoft (od wersji Windows XP w wzwyż) wykorzystywanego przez Zamawiającego ?

Zamawiający potwierdza konieczność ochrony systemów z rodziny Microsoft Windows [z Windows Server włącznie!] i pakietów biurowych Office.

19. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wskazał wymagania w zakresie usługi Antymalware. Zwracamy uwagę, że w specyfikacji brak jest wymagań technicznych parametryzujących wydajność systemu bezpieczeństwa Sandbox, uniemożliwia to prawidłowe dobranie usługi. W związku z powyższym czy Zamawiający zaakceptuje rozwiązanie umożliwiające realizacje usługi Antymalware spełniającej poniższe wymogi w zakresie wydajności:

* Ilość maszyn VM uruchamianych w systemie bezpieczeństwa Sandbox, nie mniej niż 8;
* Skanowanie AV, nie mniej niż 5000 plików/godzinę;
* Skanowanie VM, nie mniej niż 150 plików/godzinę.

Zamawiający zaakceptuje powyższe rozwiązanie.

20. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.1 Informacje ogólne – Zamawiający stawia wymaganie w brzmieniu: „Wszystkie punkty dostępowe zostaną rozmieszczone na terenie oraz wokół poszczególnych

budynków urzędów administracji samorządowej biorącej udział w projekcie oraz wybranych lokalizacjach na terenie miejscowości” . Jednocześnie z opisu urządzeń zawartego w pkt. 6.3.3 „Wymagania minimalne punktów dostępowych” wynika, iż urządzenia są urządzeniami klasy „outdoor” tj. przeznaczonymi do instalacji na otwartej przestrzeni i wystawionymi na działania czynników atmosferycznych. Zwracamy uwagę, iż instalacja punktów dostępowych wyłącznie na zewnątrz budynków lub otwartym terenie w zależności od tłumienia elewacji oraz sposobu montażu urządzeń względem ścian lub stropów budynków może znacząco wpłynąć na propagacje sygnału a co za tym idzie dostępność usługi WiFi dla użytkowników przebywających w samym budynku. W związku z powyższym czy Zamawiający zaakceptuje fakt, iż usługa WiFi może być dostępna tylko punktowo w pewnych obszarach budynków bez możliwości zapewnienia gwarantowanego pokrycia na terenie całego budynku lub nawet obszaru danego piętra ? Zwracamy uwagę, że w przypadku wymagania zapewnienia pokrycia sygnałem radiowym o zadanych parametrach całej przestrzeni biurowej dla użytkowników wewnętrznych może być wymagane przeprowadzenie instalacji punktów dostępowych klasy „in-door” tj. wewnętrznych odpowiedzialnych wyłącznie za obsługę sygnału wewnątrz budynków użyteczności publicznej. Zapewnienie pełnego pokrycia obiektów lub ściśle wyznaczonych obszarów wyspowych będzie każdorazowo wymagać przeprowadzenia pomiarów i analizy propagacji fal radiowych tzw. site survey a na koniec strojenia (tuning) danego rozwiązania WiFi co jest możliwe wyłącznie w przypadku zastosowania rozwiązań zarządzanych centralnie tj. z wykorzystaniem kontrolera sieci WLAN.

Zamawiający nie stawia wymogów w zakresie dostępności sygnału WiFi wewnątrz budynków. Jednocześnie Zamawiający po dodatkowych uzgodnieniach zmienił wymagania i obecnie wymaga dostarczenia 12 szt. AP w obudowach outdoor i 78 w obudowach indoor

21. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.1 Informacje ogólne – Zamawiający stawia wymaganie w brzmieniu: „Punkty te pozwolą na dostęp do zasobów teleinformatycznych oraz usług elektronicznych uruchomionych w ramach projektu użytkownikom korzystającym z urządzeń mobilnych, zarówno pracownikom administracji samorządowej, jak również klientom administracji” przy czym wymaganie w zakresie w/w punktów jest opisane jako: „Instalacja, konfiguracja i uruchomienie publicznych punktów”.

Prosimy o potwierdzenie, iż specyfikowane punkty dostępowe maja służyć wyłącznie jako „punkty publiczne” w zakresie dostępu do sieci internet zarówno dla użytkowników publicznych jak i pracowników Zamawiającego z wykorzystaniem technologii LTE/4G a nie realizować równocześnie funkcjonalność dostępu do zasobów sieci wewnętrznej dla pracowników Zamawiającego co wymagało by równoległego podłączenia urządzeń do sieci LAN Zamawiającego przez wymagane w tym celu okablowanie strukturalne oraz rozdzielnia funkcji transmisji danych na transmisje „internetową” przez sieć LTE/4G i „służbową” przez sieć LAN Zamawiającego. Zwracamy uwagę, iż wymaganie w zakresie równoległego przetwarzania ruchu internetowego jaki LAN jest domeną urządzeń klasy router a nie access-point (punkt dostępowy).

W przypadku potwierdzenia wymagania podłączenia punktów dostępowych do sieci LAN (ethernet) Zamawiającego prosimy o informacje czy Zamawiający zapewni niezbędne okablowanie strukturalne (miedziane bądź światłowodowe) jak i niezbędny styk (port Ethernet ze złączem RJ45) umożliwiające podłączenie punktu dostępowego do sieci LAN Zamawiającego.

Wymagane jest zapewnienie transmisji do portalu E-usług za pomocą sieci LTE/3G. Ze względów bezpieczeństwa żaden z punktów nie będzie przyłączany bezpośrednio do sieci LAN Zamawiającego uruchomionej w ramach tego projektu.

22. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.2 Miejsce instalacji punktów. Zamawiający w Tabeli nr 18 „Przewidywane miejsca instalacji punktów WiFi” specyfikuje miejsca instalacji punktów dostępowych wskazując w sumie na konieczność instalacji 53 urządzeń tego typu. Jednocześnie w Tabeli nr 1 "Ramowy wykaz dostarczanych rozwiązań do poszczególnych Partnerów Projektu" Zamawiający wskazuje 9 lokalizacji, dla których należy dostarczyć zestawy punktów dostępowych PublicWifi, gdzie Zamawiający wskazuje, iż każdy zestaw składa się z 10 sztuk AP. W związku z powyższym prosimy o wskazanie ile urządzeń typu punkt dostępowy ma zostać dostarczonych tj. 53 czy 90 szt.

Zamawiający wymaga dostarczenia 12 szt. AP w obudowach outdoor i 78 w obudowach indoor.

23. Dotyczy pkt. 6.3.3 Wymagania minimalne punktów dostępowych – w kontekście wymagania w brzmieniu: „Wymagane jest dostarczenie z punktami zestawu montażowego wraz z przewodami i patchcordami, zasilaczami, antenami i innymi akcesoriami wymaganymi do uruchomienia i prawidłowego działania systemu” prosimy o potwierdzenie, że Zamawiający wymaga by oferowane urządzenie posiadało zewnętrzne anteny radiowe.

Zamawiający wymaga aby zainstalowane punkty zapewniały dostęp do siecina możliwie jak największym obszarze. Jeśli oferowane przez Wykonawcę urządzenie będzie posiadało wbudowane anteny rekomendowane przez producenta do pracy z tym urządzeniem, Zamawiający nie będzie wymagał dostarczenia anten zewnętrznych. W każdym innym przypadku należy zainstalować anteny zewnętrzne.

24. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.3 Wymagania minimalne punktów dostępowych – w kontekście wymagania w brzmieniu: „Wymagane jest dostarczenie z punktami zestawu montażowego wraz z przewodami i patchcordami, zasilaczami, antenami i innymi akcesoriami wymaganymi do uruchomienia i prawidłowego działania systemu” prosimy o wyjaśnienie w jaki sposób ma zostać zasilone każde z urządzeń w miejscu przewidzianym do instalacji tj. z wykorzystaniem zasilania AC, DC czy power-injectora ? Jednocześnie prosimy o wyjaśnienie czy Zamawiający we własnym zakresie zapewni niezbędne źródło zasilania (gniazdo zasilania 230V, siłownie DC z wyprowadzonymi zaciskami, medium umożliwiające prowadzenie zasilania w standardzie PoE/PoE+) we wskazanym standardzie i w miejscu przewidzianym do instalacji każdego z urządzeń pełniących role punktów dostępowych (Tabela 18) ?

Zamawiający zapewni źródło zasilania 230V w miejscu instalacji punktu.

25. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.3 Wymagania minimalne punktów dostępowych – w kontekście wymagania w brzmieniu: „Wymagane jest dostarczenie z punktami zestawu montażowego wraz z przewodami i patchcordami, zasilaczami, antenami i innymi akcesoriami wymaganymi do uruchomienia i prawidłowego działania systemu” i lokalizacje wskazane do instalacji (Tabela nr 18) prosimy o wyjaśnienie czy miejsca wskazane do instalacji punktów dostępowych (budynki, ich elewacje, inne) objęte są opieką konserwatora zabytków a jeśli tak to prosimy o informacje:

 - ilu i których lokalizacji dotyczy taka sytuacja ?

Wspomniana sytuacja dotyczy 4 punktów w JST Ryn, 1 punktu w JST Mikołajki. Wszystkie wewnątrz budynków.

 - czy Zamawiający posiada tytuły prawne do wszystkich lokalizacji na których przewidziana jest instalacja wspomnianych urządzeń ?

TAK

- czy Zamawiający zobowiązuje się uzyskać wszystkie zgody konserwatora zabytków na umieszczenie urządzeń wchodzących w skład zamówienia w sytuacjach gdzie taka zgoda była by wymagana ?

TAK

26. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.3 Wymagania minimalne punktów dostępowych – w kontekście wymagania w brzmieniu: „Wymagane jest dostarczenie z punktami zestawu montażowego wraz z przewodami i patchcordami, zasilaczami, antenami i innymi akcesoriami wymaganymi do uruchomienia i prawidłowego działania systemu” i zestawienia lokalizacji przewidzianych do instalacji (Tabela nr 18), prosimy o wyjaśnienie czy w przypadku jeśli Zamawiający nie zapewni we własnym zakresie niezbędnego źródła zasilania przenosząc w tej materii odpowiedzialność na Wykonawcę czy Zamawiający weźmie odpowiedzialność za zapewnienie wszelkich uzgodnień formalnych (w tym ewentualne uzgodnienia z konserwatorem zabytków), zezwoleń prawnych związanych z montażem i eksploatacją urządzeń jak i doprowadzeniem do nich zasilania z najbliższego dostępnego w sąsiedztwie źródła.

TAK

27. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.3 Wymagania minimalne punktów dostępowych ” , zestawienia lokalizacji przewidzianych do instalacji (Tabela nr 18) oraz wymagania wyszczególnionego w Tabeli nr 3 (Zakres 1) w zakresie uruchomienia publicznych punktów dostępowych WiFi. Zwracamy się z prośbą o potwierdzenie, że Zamawiający będzie wspierał i współdziałał z Wykonawcą w uzyskaniu wszystkich niezbędnych zgód i pozwoleń jakie mogą być wymagane w zakresie w/w wymagań. Wskazujemy, że ewentualna wymagana procedura uzgodnień (odbywająca się np. z udziałem konserwatora zabytków ) może powodować przedłużenie procesu wykonania prac określonych w Zakresie 1 (max., czas 4 miesiące) z przyczyn nie leżących po stronie Wykonawcy i pomimo dochowania przez niego należytej staranności.

Zamaiający potwierdza, że Zamawiający będzie wspierał i współdziałał z Wykonawcą w uzyskaniu wszystkich niezbędnych zgód i pozwoleń jakie mogą być wymagane w zakresie w/w wymagań.

28. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.3 Wymagania minimalne punktów dostępowych – w kontekście wymagania w brzmieniu: „Wymagane jest dostarczenie z punktami zestawu montażowego wraz z przewodami i patchcordami, zasilaczami, antenami i innymi akcesoriami wymaganymi do uruchomienia i prawidłowego działania systemu” prosimy o wyjaśnienie na maksymalnie jakiej wysokości instalowane będą urządzenia pełniące rolę punktów dostępowych w miejscach jakie wyznaczył Zamawiający ? Ile z tych urządzeń będzie instalowane na wysokości powyżej 3m ?

Wszystkie urządzenia instalowane będą na wysokości ponżej 3 m.

29. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.3 Wymagania minimalne punktów dostępowych – w kontekście wymagania w pkt. 5 w brzmieniu: „Punkt musi obsługiwać protokoły i funkcje sieciowe min. w zakresie: Virtual Server and DMZ” . Zwracamy się z prośbą o uchylenie w/w wymagania. Funkcjonalność DMZ z punktu widzenia roli jaką realizuje urządzenie klasy access-point jak i funkcjonalności publicznego hot-spotu jakiej oczekuje Zamawiający jest nie zrozumiała i niczym nie uzasadniona. Urządzenie typu access-point nie jest urządzeniem klasy firewall odpowiedzialnym za kreowanie różnych stref (wewnętrznej, zewnętrznej, DMZ) z wykorzystaniem różnych interfejsów LAN zatem wymóg ten całkowicie bezzasadny.

Zamawiający zezwala na dostarczenie urządzenia nie posiadającego w/w funkcjonalności.

30. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.3 Wymagania minimalne punktów dostępowych – w kontekście wymagania w pkt. 2, podpunkt 7.

Czy Zamawiający zaakceptuje rozwiązanie gdzie funkcjonalność modułu transmisyjnego LTE/4G będzie realizowana na odrębnym, zewnętrznym urządzeniu podłączonym w bezpośrednim sąsiedztwie punktu dostępowego, spełniającym wymagania klasy IP67? Zwracamy uwagę, iż wymagania w zakresie jak przedstawił je Zamawiający (moduł LTE, wbudowany firewall) dla urządzenia typu access-point są praktycznie nie spotykane u żadnego z czołowych producentów rozwiązań tego typu przewidzianych do instalacji na otwartym powietrzu. Podtrzymanie tego wymagania skutkować będzie koniecznością poszukiwania rozwiązania niszowego producenta z Dalekiego Wschodu o wątpliwych parametrach technicznych, praktycznie nie istniejącego dotychczas na rynku polskim. Ze względu na fakt, iż urządzenia te będą pełniły role publicznych access-pointów oraz będą pracowały w warunkach atmosferycznych w reżimie całodobowym i zainstalowane będą w miejscach trudno dostępnych i wymagających specjalizowanego sprzętu do prac wysokościowych muszą spełniać wymagania w zakresie wysokich parametrów architektury rozwiązania WiFi praz parametrów MTBF (Mean Time Between Failures) co skutkuje koniecznością wykorzystania rozwiązań producentów posiadających udokumentowane i wieloletnie doświadczenia w zakresie oferowania rozwiązań WiFi klasy outdoor.

Zamawiający zaakceptuje zaoferowane rozwiązanie pod warunkiem zapewnienia pracy całego zestawu urządzeń w realnych warunkach atmosferycznych występujących na naszej szerokości geograficznej.

31. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.3 Wymagania minimalne punktów dostępowych – w kontekście wymagania w pkt. 3, podpunkt 10. Zwracamy się z prośbą o usunięcie wymagania w zakresie WDS. Funkcjonalność pracy w tym trybie wydaje się niczym nie uzasadniona w świetle wymogu zapewnienia każdemu z urządzeń bezpośredniej komunikacji poprzez sieć LTE/4G przy czym znacząco zawęża portfolio dostępnych rozwiązań.

Zamawiający zezwala na dostarczenie urządzenia nie posiadającego w/w funkcjonalności.

32. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.3 Wymagania minimalne punktów dostępowych – w kontekście wymagania w pkt. 3, podpunkt 7. Czy Zamawiający zaakceptuje zmianę wymaganego pasma dla częstotliwości 2.4GHz z 300 na co najmniej 450Mbps ? Parametr ten stoi w znaczącej dysproporcji dla wymagania wynoszącego aż 1.7Gbps dla pasma 5Ghz. Typowe parametry dla rozwiązania klasy Wave2 zaczynają się od wielkości 450Mbps dla radia 2.4GHz.

Zamawiający określił parametr minimalny na poziomie 300 Mbps. Tj: zaoferowanie urządzenia pracującego z prędkością maksymalną na poziomie 450Mbps nie spowoduje odrzucenia oferty, zaoferowanie urządzenia pracującego z prędkością maksymalną na poziomie 100 Mbps spowoduje odrzucenie oferty.

33. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.3 Wymagania minimalne punktów dostępowych – w kontekście wymagania w pkt. 6 w brzmieniu: „Urządzenie musi posiadać wbudowany mechanizm testu połączenia zarówno warstwy fizycznej jak i logiczne”. Zwracamy się z prośbą o usunięcie tego wymagania. Wymaganie to jest charakterystycznie dla rozwiązań klasy router a nie access-point i nie jest implementowane przez czołowych producentów rozwiązań WiFi za wyjątkiem niszowych producentów adaptujących niezarządzane centralnie rozwiązania klasy router do funkcji urządzenia WiFi.

Zamawiający wprowadzi zmiany w SIWZ w tym zakresie.

34. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.3 Wymagania minimalne punktów dostępowych – w kontekście wymagania w pkt. 5. Czy Zamawiający zaakceptuje rozwiązanie w którym funkcjonalności opisane w punkcie 5 zostaną zapewnione poprzez integracje punktu dostępowego z wykorzystaniem komponentu scentralizowanego kontrolera sieci WLAN (pracującego w architekturze wysokodostępnej HA) jaki planuje zaoferować Wykonawca ?

Zamawiający zaakceptuje w/w rozwiązanie.

35. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.3 Wymagania minimalne punktów dostępowych – w kontekście wymagania w pkt. 4, podpunkt 2,3.

Czy Zamawiający zaakceptuje rozwiązanie w którym funkcjonalności opisane w/w podpunktach zostaną zapewnione poprzez integracje punktu dostępowego z wykorzystaniem komponentu scentralizowanego kontrolera sieci WLAN (pracującego w architekturze wysokodostępnej HA) jaki planuje zaoferować Wykonawca? Jednocześnie zwracamy uwagę, iż architektura firewall klasy Stateful Packet Inspection czyli firewalla warstwy 4 nie pozwala obecnie skutecznie zabezpieczyć urządzenia jak i korzystających z niego użytkowników. Rozwiązaniem takim jest implementacja rozwiązania firwall klasy NGFW (nowej generacji) zapewniającym szczegółową kontrolę aplikacji, funkcjonalność Intrusion Prevention, ochroną antywirusową, blokadę komunikacji z sieciami Botnet i element szczególnie istotny w przypadku publicznych hotspotów czyli filtracje i klasyfikacje adresów URL.

Zamawiający zaakceptuje w/w rozwiązanie.

36. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.3 Wymagania minimalne punktów dostępowych – w kontekście wymagania w pkt. 4, podpunkt 5. Czy Zamawiający potwierdza, że wymaganie w zakresie URL Filteringu dotyczy funkcjonalności klasyfikacji stron URL ze względu na poszczególne grupy tematyczne a nie ze względu na prymitywna filtracje nazw domenowych lub wyrażeń regularnych w adresach URI ? Zwracamy uwagę że część rozwiązań opisywanych jako URL Filtering pozwala na bardzo prymitywną filtracje tylko w oparciu o filtracje adresów URI bez identyfikowania i przynależności adresów domenowych do poszczególnych kategorii powstałych na bazie klasyfikacji ze względu na treści. W przypadku rozwiązań publicznych hot-spotów rozwiązanie na bazie filtracji URI wydają się całkowicie nie wystarczające z punktu widzenia kontroli nad użytkownikiem końcowym i ryzyka związanego z koniecznością przekazania przedstawicielom wymiaru sprawiedliwości i służbom specjalnym informacji w przypadku zaistnienia podejrzenia popełnienia przestępstwa w wyniku wykorzystania publicznego dostępu do sieci internet.

Zamawiający potwierdza w/w zapis.

37. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.3.3 Wymagania minimalne punktów dostępowych – w kontekście wymagania w pkt. 4 (podpunkt 2-6) , pkt. 5, ze szczególnym uwzględnieniem wymagań opisanych w pkt. 11 dotyczących zapewnienia możliwości zdalnego zarządzania zwracamy się z prośbą o dopuszczenie rozwiązania punktów dostępowych zapewniających możliwość scentralizowanego zarządzania z wykorzystaniem funkcjonalności redundantnego kontrolera zarządzającego rozwiązaniem WLAN. Zwracamy uwagę że przy skali rozwiązania jakie specyfikuje Zamawiający zarzadzanie taką ilością urządzeń z jednoczesną kontrolą dostępu do internetu przez użytkowników jest praktycznie nie wykonywalne. Bez zastosowania scentralizowanej architektury zarządzani siecią WLAN nie istnieje możliwość monitorowania i logowania aktywności użytkowników korzystających z publicznych, ogólnodostępnych rozwiązań typu hot-spot. Jest to szczególnie istotne jeśli w wyniku korzystania z publicznej sieci WLAN dojdzie do próby popełnienia przestępstwa przesz korzystających z takiej sieci użytkowników. Zgodnie z obowiązującymi przepisami zarówno Policja jak i pozostałe organy państwowe w tym służby specjalne mają prawo wystąpić do usługodawcy z żądaniem dostarczenia szczegółowych danych o aktywności użytkowników jak i zasobach z jakich w internecie korzystał podejrzany. Dostarczenie takich informacji bez posiadania scentralizowanego rozwiązania w postaci redundantnego kontrolera WLAN z zaimplementowaną, aktywną funkcjonalnością co najmniej w zakresie kontroli aplikacji jak i szczegółowej filtracji URL z wykorzystaniem klasyfikacji URL a nie prymitywnych filtracji per domena czy wyrażenie regularne, zdolnego do zarządzania wszystkimi urządzeniami dostępowymi jest praktycznie niewykonalne.

Zamawiający zaakceptuje w/w rozwiązanie.

38. Dotyczy Załącznika nr 2 do SIWZ, pkt. 7 Zakres 2. Dostawa Systemów EOD, Szyn Danych lokalnych i centralnej wraz z zestawem konektorów oraz Portalu Usług Elektronicznych , 7.1 System EOD (EZD PUW) EZD PUW – pozyskanie i wdrożenie systemu nie jest przedmiotem zamówienia. Zamieszczona dokumentacja interfejsu EZD służy jedynie zdefiniowaniu parametrów i zasad wymiany danych pomiędzy portalem E-usług i systemem EZD PUW.

i 7.4. Wdrożenie EOD, integracji i Lokalnych Szyn Danych

Wdrożenie ma na celu przeprowadzenie procesu umożliwiającego każdemu z partnerów korzystanie z lokalnej infrastruktury systemowej.

i

|  |  |
| --- | --- |
| Zakres 2 | Dostawa Systemów EOD (z wyłączeniem dostawy EZD PUW) oraz Szyny Danych wraz z zestawem konektorów u każdego z partnerów projektu na poziomie lokalnym. Dostawa portalu Usług elektronicznych oraz Szyny Danych na poziomie centralnym |

Prosimy o doprecyzowanie zakresu projektu w kontekście dostawy i wdrożenia EOD. Obecne zapisy nie pozwalają na jednoznaczne określenie czy system EOD jest przedmiotem wdrożenia czy też nie. Jeżeli jest prosimy o udostępnienie wymagań serwerowych dla systemu EZD PUW.

Zamawiający pozyska i uruchomi System EZD PUW we własnym zakresie, na serwerach dostarczonych przez Wykonawcę. W zakresie Wykonawcy będzie integracja Systemu EZD PUW za pomocą zestawu konektorów zgodnie ze standardem opisanym w „Załącznik nr 8 do SIWZ - EZD API” z portalem e-usług, umożliwiającym dokonywanie e-płatności oraz komunikowanie się z platformą epuap.

39. Dotyczy Załącznika nr 2 do SIWZ, pkt. 7.3. Usługi udostępnione dla poziomu centralnego

W celu dostarczenia zaawansowanych usług elektronicznych dla mieszkańców i przedsiębiorców obszaru Wielkich Jezior Mazurskich konieczne jest dostarczenie usług integracji EOD i SD na potrzeby Portalu Usług Elektronicznych.

Czy przedmiotem projektu jest integracja SD z Portalem Usług Elektronicznych? Czy tylko przygotowanie portalu do integracji z istniejącymi systemami SD? Jeżeli integracja jest przedmiotem projektu wnosimy o wykaz partnerów projektu z podziałem na posiadane/wdrożone moduły SD. Ponadto prosimy o informację czy SD partnerów projektu są przygotowane do integracji z Portalem Usług Publicznych (udostępniają API).

Nie dotyczy. Przedmiotem zamówienia nie jest integracja z SD

40. Dotyczy Załącznika nr 2 do SIWZ pkt. 8 Zakres 3. Dostarczenie i wdrożenie formularzy elektronicznych

Prosimy o udostępnienie istniejących formularzy w formacie pdf lub doc na potrzeby oszacowania kosztów wytworzenia formularzy elektronicznych. Ponadto prosimy o wskazanie w których formularzach mają być zastosowane walidacje pól oraz pola auto wyliczalne. Jeżeli nie jest możliwe udostępnienie formularzy wnosimy o informację ile średnio stron A4 i pól posiada danych formularz.

Dostarczenie wszystkich formularzy w formacie elektronicznym na dzień dzisiejszy nie jest możliwe, należy posłużyć się wzorami dostępnymi w CRWD.

41. Dotyczy Załączniku nr 2 do SIWZ, pkt. 7.4, 9.8, Zamawiający pisze: „*Wykonawca musi działać w oparciu o system zarządzania jakością zgodny z wymaganiami ISO 9001 wydany przez jednostkę akredytowaną w zakresie projektowania, wdrażania i utrzymywania oprogramowania wspomagającego pracę jednostek administracji publicznej lub równoważny oraz w oparciu o system zarządzania jakością zgodny z wymaganiami ISO/IEC 27001 wydany przez jednostkę akredytowaną w zakresie projektowania, wdrażania i utrzymywania oprogramowania wspomagającego pracę jednostek administracji publicznej lub równoważny."* Wykonawca zwraca uwagę, iż zapisy z wymaganiami ISO odnoszą się do warstwy oprogramowania, natomiast nie są wymagane co do IaaS (Lokalizacji Centralnej). Czy intencją Zamawiającego jest by dostarczona przez Wykonawcę platforma IaaS również musi byś posadowiona w obiektach posiadających certyfikaty ISO 9001, oraz ISO/IEC 27001?

W ramach usługi serwisu Wykonawca będzie musiał świadczyć usługę wsparcia dla oprogramowania, w tym zakresie należy rozumieć postawione wymagania.

42. Dotyczy Załącznika nr 2 do SIWZ, pkt. 7.4, 9.8 SzOPZ na str: 46 ma brzmienie:

„Wykonawca musi działać w oparciu o system zarządzania jakością zgodny z wymaganiami ISO 9001 wydany przez jednostkę akredytowaną w zakresie projektowania, wdrażania i utrzymywania oprogramowania wspomagającego pracę jednostek administracji publicznej lub równoważny oraz w oparciu o system zarządzania jakością zgodny z wymaganiami ISO/IEC 27001 wydany przez jednostkę akredytowaną w zakresie projektowania, wdrażania i utrzymywania oprogramowania

wspomagającego pracę jednostek administracji publicznej lub równoważny. W przytoczonym punkcie Zamawiający wymaga certyfikatów ISO w zakresie projektowania, wdrażania i utrzymywania oprogramowania Czy poprawną interpretacja jest iż wspomniane certyfikaty wymagane są również w stosunku do DataCenter w którym zlokalizowany jest IaaS Wykonawcy (w SIWZ opisane jako Lokalizacja Centralna) ?

Czy Zamawiający wymaga dostarczenia wymienionych certyfikatów ISO ?

Zamawiający nie wymaga dostarczenia certyfikatów, jednakże zastrzega sobie prawo do kontroli wy tym zakresie w każdym momencie po i przed podpisaniem umowy.

43. Dotyczy Załącznika nr 2 do SIWZ, pkt. 2.1 Zarys rozwiązania, Tabela 1. Ramowy wykaz dostarczanych rozwiązań do poszczególnych Partnerów Projektu na str. 5 Zamawiający wskazuje dla poszczególnych lokalizacji ilości przełączników 48 portowych.

Dla lokalizacji Urząd Miejski w Węgorzewie, Urząd Miasta i Gminy Mikołajki, Urząd Miasta i Gminy Ryn, Urząd Miejski w Orzyszu, Urząd Gminy Miłki, oraz Urząd Gminy Pozezdrze wskazano po jednym przełączniku 48 port co uniemożliwia zbudowanie architektury HA (wysokiej dostępności) dla serwerów do których będą się łączyć PC i urządzenia peryferyjne.

Czy Zamawiający wymaga dostarczenia rozwiązań wysokiej dostępności w wszystkich lokalizacjach ?

TAK

Czy intencją Zamawiającego w przedstawionej tabeli jest minimalna ilość portów na przełączników dla urządzeń końcowych/peryferyjnych Zamawiającego ?

TAK

Intencją Zamawiającego, zgodnie z pkt „WSZL20” pkt 6.1.1, jest stworzenie bezpiecznego i szybkiego środowiska do pracy systemów informatycznych Zamawiającego. Podane w tabeli ilości przełączników są minimalną ilością dostarczaną w ramach projektu. Zgodnie z pkt WSZL20 to na Wykonawcy ciąży obowiązek zapewnienia odpowiedniego poziomu bezpieczeństwa. Jeżeli Wykonawca uzna, że zawarta w tabeli liczba wystarczy, nie musi uwzględniać w ofercie dodatkowych przełączników, jeśli uzna, że należy w ofercie uwzględnić więcej przełączników [np. FC czy FCoE wyłącznie do podłączenia serwerów z macierzami lub serwerów z siecią LAN, itp..] to Zamawiający dopuści takie rozwiązanie.

44. Dotyczy Załącznika nr 2 do SIWZ, pkt. pkt 2.1 Zarys rozwiązania, Tabela 1. Ramowy wykaz dostarczanych rozwiązań do poszczególnych Partnerów Projektu na str. 5 Zamawiający wskazał na dostarczenie "Motor bazy danych Microsoft®SQL Express / lub równoważny funkcjonalnie kompatybilny z systemem EOD".

Czy Zamawiający dysponuje licencjami Windows Serwer umożliwiającymi uruchomienie Microsoft®SQL Express czy dostarczenie licencji leży po stronie Wykonawcy ?

Dostarczenie licencji jest częścią projektu i leży po stronie Wykonawcy.

45. Dotyczy Załącznika nr 2 do SIWZ, pkt. 3 Określenie Przedmiotu Zamówienia w Tabela 3 Ramowe zestawienie zakresu przedmiotu zamówienia na str. 12 , Zakres 2 - Dostawa Systemów EOD (z wyłączeniem dostawy EZD PUW) oraz Szyny Danych wraz z zestawem konektorów u każdego z partnerów projektu na poziomie lokalnym. Dostawa portalu Usług elektronicznych oraz Szyny Danych na poziomie centralnym.

oraz pkt 7.1 System EOD (EZD PUW) na str. 44 oraz pkt 6.1.1, Wymagania ogólne dot. dostarczanego sprzętu , Tabela 5 Wymagania ogólne dot. dostarczanego sprzętu na str. 18 , kod: WSZL19

"Zamawiający wymaga uruchomienia na serwerach fizycznych maszyn wirtualnych realizujących następujące zadania: Kontroler AD, serwer pocztowy, serwer EZD + innych niezbędnych do pracy całości komponentów [np. DNS, DHCP, NTP] w oparciu o oprogramowanie do wirtualizacji o parametrach minimalnych określonych w rozdziale 6.1.8" z zamówienia wyłączono dostawę EZD PUW autorstwa Podlaskiego Urzędu Wojewódzkiego w Białymstoku wraz z dokumentacją Załącznik nr 8 do SIWZ. Wykonawca nie znajduje informacji wymagań sprzętowych/wydajnościowych dla systemu EZD PUW. Czy Zamawiający wymaga zasobów pozwalających na uruchomienie systemu EZD PUW na dostarczanej infrastrukturze?

Jeśli zasoby są wymagane prosimy o wskazanie rekomendacji producenta.

Czy Zamawiający wraz z systemem EZD PUW zapewnia również licencje w zakresie systemu operacyjnego i bazy danych zapewniających prace przedmiotowego systemu ?

Zamawiający wymaga uruchomienia EZD PUW na infrastrukturze dostarczonej przez Wykonawcę w ramach tego postępowania. Do zadań Wykonawcy należy również dostarczenie licencji na systemy operacyjne.

Wymagania minimalne do pracy EZD PUW:

dla serwera aplikacji:

- min 2 core 2 GHz

- min RAM 4 GB,

- min 50 GB przestrzeni dyskowej

dla serwera bazy danych:

- min. 2 core 2 GHz

- min 8GB RAM

- min. 50 GB przestrzeni dyskowej

- MS SQL Express 2016

Obydwa serwery wymagają systemu Windows Server.

46. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.1 Dostawa sprzętu, 6.1.1 Wymagania ogólne dot. dostarczanego sprzętu, Tabela 5 Wymagania ogólne dot. dostarczanego sprzętu na str. 18, kod: WSZL16 napisano: "Serwer AD - Do lokalizacji 5,6,7,8,9,10,11 (do 50 użytkowników) Wykonawca dostarczy po min. dwa serwery fizyczne spełniające wymagania z rozdziału 6.1.3; do lokalizacji 1,2,3,4,12 (od 51-150 użytkowników) Wykonawca dostarczy po min. dwa serwery fizyczne spełniające wymagania z rozdziału 6.1.4" natomiast w pkt 6.1.3 Wymagania minimalne dotyczące serwera AD – wariant I Tabela 7 napisano; "Wymagania minimalne dotyczące Serwera Active Directory - wariant I" oraz w pkt 6.1.4 Wymagania minimalne dotyczące serwera AD – wariant II na str. 22 Tabela 8 napisano; "Wymaganie minimalne dotyczące serwera Active Directorty - wariant II".

Czy serwer AD wymagany dla poszczególnych lokalizacji jest tożsamy z wymaganiem na serwer Active Directory?

Czy opis dla Tabeli 7 i dla Tabeli 8 mówiący o Active Directorty jest omyłkowy ?

Zamawiający wymaga dostarczenia serwerów spałniających kryteria opisane w przytoczonych tabelach, których głównym zadaniem będzie pełnienie roli kontrolerów Active Directory, stąd nazwa. Wszystkie serwery zostaną oczywiście zwirtualizowane.

Opis tabeli 7 i 8 mozna w tym kontekście traktować jako omyłkowy bowiem dotyczy maszyn fizycznych.

47. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.1 Dostawa sprzętu 6.1.1 Wymagania ogólne dot. dostarczanego sprzętu, Tabela 5 Wymagania ogólne dot. dostarczanego sprzętu na str. 18, kod: WSZL21 "Zamawiający wymaga aby w lokalizacjach 1,2,3,4,12 , Wykonawca zapewnił zabezpieczenie systemu przed zanikiem napięcia sieciowego o następujących parametrach minimalnych :

• System zapewniający podtrzymanie zasilania dostarczonego rozwiązania przez czas nie krótszy niż 15 min dla całego dostarczonego środowiska sprzętowego – serwery, lub jeśli czas bezpiecznego wyłączenia systemu jest dłuższy niż 15 minut umożliwiający automatyczne i bezpieczne wyłączenie systemu. Z czasem przełączania po zaniku napięcia na wewnętrzne źródło prądu umożliwiającym ciągłą pracę serwerów i macierzy [rzędu 6ms]... "

Wykonawca zauważa, iż wymaganie określono dla 5 z 12 lokalizacji natomiast rodzi się pytanie co do pozostałych lokalizacji , czy Zamawiający dysponuje i dostarczy zabezpieczenie systemu przed zanikiem napięcia sieciowego . Należy zauważyć, iż potrzebna moc takiego zasilania będzie znana Zamawiającemu nie wcześniej niż po wyborze Wykonawcy/dostarczeniu sprzętu.

Zamawiający omyłkowo wymienił tylko niektóre lokalizacje. Zabezpiecznie przed zanikiem zasilania, zdolne podtrzymać przez min. 10 min. zasilanie routera, przełączników, serwerów i macierzy musi być dostarczone do wszytkich lokalizacji. Jest to traktowane jako element zabezpiczenia systemu. Moc urządzeń podtrzymujących należy obliczyć w oparciu o parametry dostarczanych przez wykonawcę elementów systemu.

48. Dotyczy Załącznika nr 2 do SIWZ, pkt. 12 Zakres 7. Świadczenie usługi serwisu str. 84

Tabela 34 Minimalny zakres prac świadczonych w ramach usługi wsparcia i serwisu,

nr WG18 , napisano: "W ramach świadczonej usługi chmurowej Wykonawca musi zapewnić usługę backupu opisaną w instrukcji backupu i archiwizacji stworzonej wspólne z Zamawiającym."

oraz

CM-Zacznik\_nr\_6\_do\_Umowy\_-\_Procedura\_serwisu, Zakres usługi serwisu i wsparcia na str. 5

Lp 6 napisano: "Utrzymanie systemu kopii bezpieczeństwa i archiwum w lokalizacji centralnej zgodnie z zapisami Procedury backupu."

Wykonawca zauważa, iż w zapisach zostało określone wymaganie tworzenia backup i archiwizacji dla usługi chmurowej (lokalizacji centralnej) oraz backup dla jednostek samorządowych.

Czy Zamawiający wymaga archiwizacji danych i systemów dla jednostek samorządowych czy tylko dla lokalizacji centralnej ?

Zamawiający wymaga aby archiwizacji i backupowi w opisany sposób poddawane były jedynie dane z systemów poszczególnych jednostek, wykonanych przez Wykonanwcę, zgodnie z procedurą stworzoną wspólnie z Wykonawcą.

49. Dotyczy Załącznika nr 2 do SIWZ, pkt. 2.1 , Zamawiający pisze: „Sieci lokalne LAN zostaną zmodernizowane do min. kategorii 5e; wszelkie prace instalacyjne związane z rozbudową sieci LAN zostaną wykonane zgodnie ze schematami zamieszczonymi w Załączniku nr 9 do SIWZ oraz w porozumieniu z lokalnymi administratorami sieci, ilość punktów elektryczno-logicznych zostanie zwiększona zgodnie z poniższą tabelą”

Prosimy o potwierdzenie, że budowa/modernizacja sieci LAN dotyczy jedynie lokalizacji: Starostwo Powiatowe w Giżycku (2 lokalizacje – dla każdej lokalizacji wymagane jest dostarczenie 61 PEL), Urząd Gminy w Giżycku, Urząd Miasta i Gminy Ruciane-Nida, Urząd Miasta i Gminy Ryn, Urząd Gminy Miłki, a wskazana w tabeli liczba PEL (do naprawy lub instalacji) jest ostateczną, docelową ilością PEL w danej lokalizacji.

„Tabela 1. Ramowy wykaz dostarczanych rozwiązań do poszczególnych Partnerów Projektu” Zawiera pozycję „Sieć elektryczno-logiczna (liczba PEL do naprawy lub instalacji)” wskazującą na ilości nowo instalowanych bądź modernizowanych punktów sieci w poszczególnych jednostkach. Wszędzie tam, gdzie wskazno „0” nie wymaga się instalacji ani modernizacji punktów.

50. Dotyczy Załącznika nr 2 do SIWZ, pkt. 2.1 , Zamawiający pisze: „Zastosowanie protokołu szyfrowanego MPLS umożliwi stworzenie zarządzanego wspólnego medium dostępowego partnerów do platformy udostępnionej w chmurze obliczeniowej (IAAS). Dla wszystkich routerów brzegowych zostanie opracowany wspólny plan adresacji zapewniający możliwość dodawania nowych JST oraz dostęp pracowników utworzonego na potrzeby projektu centrum kompetencji do zasobów teleinformatycznych każdego JST”

Prosimy o potwierdzenie, że Zamawiający nie oczekuje dodatkowego szyfrowania danych na routerach CE (ipsec) w ramach wdrożenia sieci MPLS, tylko oczekuje dostarczenia bezpiecznej, wydzielonej sieci WAN - zbudowanej na zasobach Operatora (?)

Zgodnie z SIWZ Zamawiający potwierdza, że wymaga uruchomienia tuneli IPsec na routerach CE w ramach sieci MPLS.

51. Dotyczy Załącznika nr 2 do SIWZ. Zmiana statusu wniosku złożonego przez petenta powinna wygenerować notyfikacje SMS/email.

Prosimy o określenie jaka jest szacunkowa, prognozowana ilość wiadomości SMS wygenerowanych przez wszystkie JST w ciągu jednego miesiąca ?

|  |  |
| --- | --- |
| Miasto Gizycko | 200 |
| Gmina Gizycko | 200 |
| Starostwo Gizycko | 30 |
| Miasto Mrągowo | 200 |
| Gmina Mrągowo | 100 |
| Miasto Ryn | 100 |
| Gmian Ruciane-Nida | 200 |
| Gmina Miłki | 60 |
| Gmina Pozezdrze | 100 |
| Miasto Węgorzewo | 200 |
| Miasto Orzysz | 200 |
| Miasto Mikołajki | 200 |

52. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.2.1 . Zamawiający pisze: „W lokalizacjach Zamawiającego zapewnione są warunki niezbędne do zainstalowania i pracy urządzeń a w szczególności zapewniono wymagane przez producenta warunki eksploatacji urządzeń - zamawiający musi udostępnić infrastrukturę kablową, która po modernizacji PEL spełni wymagania normy ISO/IEC 11801, ANSI/TIA/EIA-568, PN-EN 50173, Zamawiający zapewnia także zasilanie niezbędne do funkcjonowania urządzeń oraz miejsce w szafach Rack.”

Prosimy o potwierdzenie, że Zamawiający udostępni we wszystkich lokalizacjach JST miejsce w swoich szafach Rack. Prosimy o wskazanie ilości wolnego miejsca RU (rack unit) w szafach Zamawiającego w każdej lokalizacji JST.

Zamawiający potwierdza że zabezpieczy odpowiednią ilość RU w szafach – do 42 RU.

53. Prosimy o potwierdzenie, że Zamawiający nie oczekuje budowy systemu rozproszonych centrów monitoringu, tylko jeden centralny system monitoringu, który pozwala na monitorowanie całej infrastruktury (serwery, VM, sprzęt sieciowy – routery, przełączniki, access pointy i UPSy) we wszystkich JST. Każde Centrum Kompetencji Zamawiającego będzie monitorować urządzenia w swoim obszarze sieci.

Zamawiający potwierdza iż w ramach jednej z JST zamierza utworzyć Lokalne Centrum Kompetencji, którego zadaniem bedzie monitorowanie całej dostarczonej infrastruktury. Jednocześnie w każdym JST zatrudniony jest informatyk, który musi mieć mozliwość nadzorowania sieci LAN własnej jednostki JST.

54. Wykonawca prosi Zamawiającego o informację przez jaki czas mają być przez Wykonawcę przechowywane logi z systemu monitorowania sieci ? (1 rok, 2 lata, 3 lata)

Minimum w okresie 30 dni.

55. Dotyczy Załącznika nr 2 do SIWZ, pkt. 6.1.6.1 Stanowisko robocze – komputer stacjonarny i monitor „Wyposażenie dodatkowe: program antywirusowy zarządzany z centralnej konsoli”

Czy Zamawiający w ramach wymaganego oprogramowania antywirusowego wymaga także dostarczenia centralnej konsoli do zarządzania oprogramowaniem antywirusowym zainstalowanym na stacji roboczej?

Zamawiający wymaga dostarczenia oprogramowania centralnej konsoli możliwej do zainstalowania na co najmniej jednym stanowisku w każdej z lokalizacji.

56. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wskazał wymagania w zakresie usługi Ochrona przed atakami, posiadania co najmniej dwóch niezależnie działających linii wsparcia dedykowanych do obsługi wyłącznie incydentów z obszaru bezpieczeństwa. Pierwsza linia wsparcia musi pełnić funkcje monitoringu i operacyjnej ochrony przed atakami oraz prowadzić ciągły dyżur przez co najmniej dwie osoby. Druga linia wsparcia będzie realizowała funkcję poszukiwania, analizowania i rozwiązywania niestandardowych problemów związanych z obsługa incydentów w zakresie bezpieczeństwa. Czy Zamawiający dopuszcza możliwość „zależności” operacyjnej pomiędzy liniami wsparcia w zakresie analizy niestandardowych incydentów i przekazywania takich informacji pomiędzy liniami?

Zamawiający dopuszcza w/w rozwiązanie.

57. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wskazał wymagania w zakresie usługi Ochrona przed atakami, w zakresie gromadzenia informacje o wszystkich połączeniach do systemów usługowych Zamawiającego poprzez wykorzystanie protokołu typu NetFIow lub podobnych. Prosimy o udzielenie informacji czy Zamawiający wymaga składowania informacji o wszystkich połączeniach z urządzeń aktywnych? Jeżeli tak, to przez jaki okres czasu takie informacje mają być składowane i w jakiej formie?

Zamawiający wymaga składowania tych informacji przez okres co najmniej 30 dni.

58. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wskazał wymagania w zakresie usługi Ochrona przed atakami, w zakresie inspekcji ruchu w celu identyfikacji ataków przeprowadzanych na podatności payload. Prosimy o potwierdzenie, że inspekcja dotyczy tylko i wyłącznie ataków denial-of-service.

Zamawiający potwierdza w/w zapis.

59. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wskazał wymagania w zakresie usługi Ochrona przed atakami, w zakresie konieczności raportowania do Zamawiającego o każdym wykrytym ataku na infrastrukturę Zamawiającego. Czy Zamawiający dysponuje służbami technicznymi mogącymi być angażowanymi do obsługi incydentów w całodobowym trybie operacyjnym?

Zamawiający nie wymaga informowania o każdym ataku w chwili jego wykrycia a jedynie raportowania o wykrytych i powstrzymanych atakach w raportach okresowych.

60. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wskazał wymagania w zakresie usługi Ochrona przed atakami, w zakresie konieczności raportowania do Zamawiającego o każdym wykrytym ataku na infrastrukturę Zamawiającego. Czy Zamawiający przez konieczność raportowania o każdym wykrytym ataku na infrastrukturę Zamawiającego rozumie tylko i wyłącznie czynność notyfikacji/raportową?

Zamawiający nie wymaga informowania o każdym ataku w chwili jego wykrycia a jedynie raportowania o wykrytych i powstrzymanych atakach w raportach okresowych.

W ZESTAWIE BRAK PYTANIA ZE STRONY WYKONAWCY O NUMERZE 61

62. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wskazał wymagania w zakresie usługi Antymalware. Zwracamy uwagę, że w wymaganiach brak jest informacji odnośnie wspieranych plików przez Sandbox, prosimy o potwierdzenie, że zaoferowana przez Wykonawcę usługa Antymalware ma dokonywać analizy co najmniej następujących typów plików: .7z, .ace, .apk, .arj, .bat, .bz2, .cab, .cmd, .dll, .doc, .docm, .docx, .dot, .dotm, .dotx, .exe, .gz, .htm, html, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip

Zamawiający potwierdza, że powyższą listę rodzajów plików należy uznać za zakres minimalny w tym zakresie.

63. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, dla usług II. Cloud Firewall, III. Antymalware, IV. Web Application Firewall, VI. System ochrony serwerów w JST, Zamawiający wskazał wymagania w zakresie obsługi ruchu HTTPS. Prosimy o potwierdzenie, że w celu obsługi ruchu zaszyfrowanego, Zamawiający przekaże Wykonawcy dodatkowo wygenerowany klucz prywatny.

Zamawiający przekaże Wykonawcy wszystkie informacje niezbędne do prawidłowej realizacji usług zgodnie z Umową, z zastrzeżeniem, że wszystkie dane szyfrowane za pomocą protokołu HTTPS stanowią tajemnicę.

64. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wskazał wymagania w zakresie usługi Antymalware. Prosimy o potwierdzenie, że oferowana usługa ma wykrywać i blokować komunikację z adresami URL zawierającymi malware.

Zamawiający potwierdza w/w zapis.

65. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wskazał wymagania w zakresie usługi Antymalware. Prosimy o potwierdzenie, że logi z wykrytych zagrożeniach lub podejrzeniach ataków mają być udostępnione w centralnym systemie logowania i raportowania, który ma zostać dostarczony w ramach usługi Cloud Firewall.

Zamawiający potwierdza w/w zapis.

66. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wskazał wymagania w zakresie usługi Antymalware. Prosimy o potwierdzenie, czy Zamawiający wymaga wirtualnego środowiska testowego (Sandbox), przeznaczonego jedynie dla JST biorących udział w projekcie i odizolowanego od innych klientów.

Zamawiający wymaga aby Sandbox był usługą dedykowaną dla JST biorących udział w projekcie.

67. W załączniku nr 2 do SIWZ, punkt 9.6 „Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy”, cześć WD13 „Bezpieczeństwo i ochrona przed atakami”, Zamawiający wskazał wymagania w zakresie pozostałych wymagań względem Wykonawcy, w zakresie zapewnia Zamawiającemu możliwość konsultacji w języku polskim z inżynierami o specjalizacji bezpieczeństwo w wymiarze 20 godzin miesięcznie, przy czym godziny niewykorzystane w danym miesiącu sumują się z godzinami przeznaczonymi do wykorzystania w miesiącu następnym. Czy Zamawiający przewiduje, że godziny sumują się w całości kontraktu, czy tylko w obrębie miesiąca kolejnego, tj. w wymiarze maksymalnie 40 godzin w miesiącu.

Zamawiający uzna warunek za spełniony w obydwu przypadkach.

68. Zamawiający w dokumencie Opisu Przedmiotu Zamówienia, w sekcji 2.1. Zarys rozwiązania, tabela „Ramowy wykaz dostarczanych rozwiązań do poszczególnych Partnerów Projektu”. Opisuje wymaganie dotyczące oprogramowania serwera: „*Serwery [z usługami: Microsoft Windows Serwer / Active Directory / EZD, itd.]*”. Czy Zamawiający dopuszcza inne rozwiązania, bazujące na systemie Linux? Da to ten sam efekt, a jednocześnie nie graniczy dostawy rozwiązania do jednego, komercyjnego dostawcy.

Zamawiający dopuści zastosowanie systemu operacyjnego innego niż Windows Server, wymagana jest jednak możliwość uruchomienia usług MS Active Directory oraz MS SQL Server.

69. Zamawiający w dokumencie Opisu Przedmiotu Zamówienia, w rozdziale „Zakres 3. Dostarczenie i wdrożenie formularzy elektronicznych” definiuje listę formularzy, jakie trzeba wykonać na rzecz Zamawiającego. Wykonawca prosi o potwierdzenie, że chodzi jedynie o ich wykonanie oraz o umieszczenie ich na ePUAP. Zamawiający w tym rozdziale nie precyzuje innych prac lub innych wymagań dotyczących formularzy.

Wykonanie formularza to:

a) wykonanie wszystkich prac związanych z dostarczeniem tj. w szczególności: uzgodnienie przebiegu danej procedury przez Wykonawcę z Zamawiającym w oparciu o „karty usług” i indywidualne konsultacje, przygotowanie projektu e-formularza wraz z opisem jego przebiegu, przedstawienie projektu do testowania i zatwierdzenia Zamawiającemu;

b) wdrożenie czyli pełna integracja e-formularzy z poszczególnymi modułami portalu usług elektronicznych i systemem EZD PUW zgodnie z pkt. 9 Opisu Przedmiotu Zamówienia oraz umieszczenie na ePUAP u każdego z partnerów- w przypadku e-formularzy dotyczących wszystkich partnerów (nr 1-5), a w przypadku pozostałych e-formularzy w podziale na Gminy i Powiat.

Dodatkowo Wykonawca wnosi o sprecyzowanie ww. listy pod kątem formularza, jaki ma być wykonany. Obecnie Zamawiający precyzuje jedynie hasłowo pewien zakres prac. Przykład: „*Dostęp do informacji publicznej”.*

Wykonawca prosi o potwierdzenie, że chodzi o *„Wniosek o udostępnienie informacji publicznej*”.

TAK

Podobne trudności w interpretacji napotykamy w przypadku określenia „*Rozpatrywanie skarg i wniosków*”. Czy chodzi o formularz zgłoszenia skargi / wniosku?

TAK

Podobnie „*Wydawanie zaświadczeń*”, czy ma to być ogólny wniosek o wydanie zaświadczenia, czy konkretnego?

Ogólny

„*Opiniowanie projektów studium uwarunkowań*”, Czy chodzi o formularz wniosku o wydane opinii w sprawie projektu studium uwarunkowań?

TAK

Prosimy o sprecyzowanie całej listy formularzy w taki sposób, aby wskazywały na konkretny wniosek lub zgłoszenie, bez czego nie uda się dokładnie określić, co ma być wykonane.

Zamawiający poprawił treść tabeli 23 w załączniku nr 2 do SIWZ - SzOPZ.

Ewentualnie prosimy o potwierdzenie, że dla każdej pozycji z listy Zamawiający przedstawi papierowy wzór wniosku dokładnie odpowiadający określonemu formularzowi, zgodnie z wymaganiem WF2 w rozdziale „8 Zakres 3. Dostarczenie i wdrożenie formularzy elektronicznych”.

Zgodnie z wymaganiem WF2 to Wykonawca opracowuje formularz elektroniczny (zgodnie z właściwymi przepisami prawa) wykorzystując posiadane zasoby. Zamawiający po zakończeniu postępowania przedstawi wybranemu Wykonawcy tzw. „karty usług”, czyli opisy przebiegu realizowanych dotychczas procedur postępowania w jst. oraz ewentualnie stosowanych standardowych formularzy. Jednocześnie informujemy, że wszystkie wskazane e-formularze oraz opisy przebiegu procedur z nimi związanych są ogólnie dostępne na wielu portalach rządowych i samorządowych zatem Zamawiający zgodnie z wymaganiem WF14 - dopuszcza możliwość wykorzystania przez Wykonawcę wzorów, które są już opublikowane w CRD. Jak wspomniano wyżej projekty e-formularzy będą wymagały wcześniejszego przedstawienia do zatwierdzenia Zamawiającemu.

1. Zamawiający w dokumencie Opisu Przedmiotu Zamówienia, w rozdziale 9.8 Wdrożenie opisuje wymaganie „*W ramach usług wdrożeniowych, Wykonawca zrealizuje:*

*- Udostępnienie na infrastrukturze sprzętowej Zamawiającego systemu SUE wraz z centralną szyną danych na potrzeby procesu wdrożenia i szkolenia*

*- Skonfiguruje warstwę sprzętową, systemową i sieciową gwarantując odpowiedni poziom bezpieczeństwa*

*- Uzgodni i wdroży poziom bezpieczeństwa w obszarze integracji Centralnej Szyny danych z systemami urzędów Stowarzyszenia Wielkie Jeziora Mazurskie 2020*

*- Będzie dokonywał aktualizacji systemu SUE oraz konfiguracji Centralnej Szyny Danych na potrzeby realizacji projektu.*”.

Zamawiający opisuje wymóg aktualizacji sytemu SUE, jednak nie podaje, w jakim okresie ma się ona odbywać. Wykonawca prosi o potwierdzenie, że wymaganie dotyczy okresu wdrożenia.

Wymóg utrzymania, i aktualizacji SUE dotyczy okresu wdrażania oraz okresu wsparcia, tj. 60 msc, od momentu zakończenia wdrożenia.

1. Zamawiający w dokumencie Opisu Przedmiotu Zamówienia, w rozdziale „10 Zakres 5. Przygotowanie i przeprowadzenie pakietów szkoleń” opisuje, że „*oczekuje przeprowadzenia szkoleń grupowych nie więcej niż:*

*- 10 dni szkoleń z zakresu integracji w warstwie Lokalnej Szyny Danych*”.

Wykonawca prosi o potwierdzenie, że chodzi o szkolenia dla administratorów z obsługi i konfiguracji szyny danych.

Zamawiający potwierdza w/w zapis.

1. Zamawiający w dokumencie Opisu Przedmiotu Zamówienia, w rozdziale „12 Zakres 7. Świadczenie usługi serwisu”, wymaganie WG13 pisze „*Wykonawca zapewnia dostosowanie do obowiązujących przepisów nie później niż w dniu ich wejścia w życie*”. Wykonawca zwraca uwagę, że często dostosowanie oprogramowania do zmian w przepisach w dniu ich wejścia w życie jest niemożliwe ze względu na krótki okres legislacyjny, tj. uchwalanie nowych przepisów w bardzo krótkim czasie. Dlatego też Wykonawca wnosi o zmianę brzmienia tego zapisu na następujący: „*Wykonawca zapewnia dostosowanie do obowiązujących przepisów nie później niż w dniu ich wejścia w życie, chyba że zmiany prawne nie zostały ogłoszone z minimum 30-dniowym terminem poprzedzającym ich wprowadzenie w życie. W przypadku, jeżeli zmiany nie zostały ogłoszone z minimum 30-dniowym terminem poprzedzającym ich wprowadzenie w życie, Wykonawca zobligowany jest do ich wprowadzenia w ciągu 30 dni roboczych od dnia wprowadzenia przepisu w życie.*”.

Dodatkowo Wykonawca zauważa, że w § 12 USŁUGI UTRZYMANIA Zamawiający precyzuje w ust. 5.3 „*dokonywanie zmian w Oprogramowaniu Dedykowanym, nie wynikających z nieprawidłowego działania Oprogramowania, a wynikających ze zmiany obowiązującego prawa w terminie 30 dni od dnia otrzymania przez Wykonawcę pisemnego zlecenia od Zamawiającego; zmiany w Oprogramowaniu Dedykowanym będą dotyczyły zmian wynikających z obowiązujących przepisów prawnych opublikowanych w Dzienniku Ustaw RP oraz w Dzienniku Urzędowym RP „Monitor Polski”, a także zmian prawa lokalnego i procedur wewnętrznych obowiązujących w jednostce Zamawiającego oraz dotyczyć będą funkcjonalności istniejących i wdrożonych u Zamawiającego zgodnie z Umową.*”. Wychodzi na to, że dwa wskazane paragrafy w tym samym wzorze umowy stoją ze sobą w sprzeczności odnośnie zapisów o dostosowaniu do zmian w przepisach prawa. Wykonawca wnosi o ujednolicenie tych zapisów zgodnie z propozycją Wykonawcy.

Zamawiający zgodzi się na wprowadzenie proponowanych zmian.

1. Zamawiający w dokumencie wzoru umowy, § 11 GWARANCJA, ust. 10.1. pisze „*Czasy wskazane w Załącznik nr 6 do Umowy liczone są od chwili dokonania zgłoszenia.*”. Tymczasem w dokumencie Opisu Przedmiotu Zamówienia, rozdział „12 Zakres 7. Świadczenie usługi serwisu” Zamawiający opisuje „*Wykonawca zobowiązany jest do potwierdzenia w ciągu 4 godzin w czasie okna dostępności usługi serwisowej przyjęcie Zgłoszenia reklamacyjnego oraz jego klasyfikację. Potwierdzenie zostanie wysłane przez Wykonawcę do zgłaszającego.*”. Obydwa zapisy są ze sobą sprzeczne. Zapis z Opisu Przedmiotu Zamówienia mówi o tym, że Wykonawca ma 4 godziny na potwierdzenie rejestracji zgłoszenia i nadania mu kategorii. Logiczne jest, że czas naprawy dysfunkcji rozpoczyna się od momentu potwierdzenia rejestracji zgłoszenia i nadania mu kategorii. Tymczasem we wzorze umowy Zamawiający wymaga liczenia czasu naprawy od momentu wykonania zgłoszenia, mimo braku potwierdzenia jego zarejestrowania i mimo braku nadania jakiejkolwiek kategorii. Wykonawca wnosi o korektę zapisów wzoru umowy na takie, które są zgodne z Opisem Przedmiotu Zamówienia. Wykonawca proponuje następujący zapis: „*Czasy wskazane w Załącznik nr 6 do Umowy liczone są od chwili potwierdzenia zgłoszenia przez Wykonawcę i nadania mu kategorii*”.

Podobnie w ust. 10.2. Zamawiający pisze „*Zamawiający może dokonać zgłoszenia za pomocą innych kanałów komunikacji uzgodnione pomiędzy Stronami, a zgłoszenie dokonane za pomocą każdego z nich jest uznawane za dokonane skutecznie z chwilą, gdy zgłoszenie dotarło do Wykonawcy lub zostało wprowadzone do środka komunikacji elektronicznej w taki sposób, że Wykonawca mógł zapoznać się z jego treścią.*”. W tym wypadku również Zamawiający pominął czas, jaki ma Wykonawca na potwierdzenie zgłoszenia i nadanie mu kategorii. Wykonawca prosi o korektę tych zapisów na takie, które są zgodne z Opisem Przedmiotu Zamówienia. Wykonawca proponuje następujący zapis: „*Zamawiający może dokonać zgłoszenia za pomocą innych kanałów komunikacji uzgodnionymi pomiędzy Stronami, a zgłoszenie dokonane za pomocą każdego z nich jest uznawane za dokonane skutecznie z chwilą, gdy zgłoszenie dotarło do Wykonawcy lub zostało wprowadzone do środka komunikacji elektronicznej w taki sposób, że Wykonawca mógł zapoznać się z jego treścią, następnie Wykonawca potwierdził jego rejestrację i nadał mu kategorię.*”.

Wykonawca zwraca uwagę, że ujednolicenia wymaga także punkt 4 dokumentu Procedury Serwisowej, który brzmi „*Zgłoszenie Serwisowe realizowane drogą internetową uznaje się za dokonane z chwilą wpłynięcia na adres poczty elektronicznej podany w Zgłoszeniu Serwisowym do Zamawiającego potwierdzenia przyjęcia zgłoszenia serwisowego – potwierdzenie wysyłane jest automatycznie*”. Zapis ten również stoi w sprzeczności z zapisem Opisu Przedmiotu Zamówienia, który daje 4 godziny na potwierdzenie i kategoryzację zgłoszenia.

Zamawiający wprowadził zmiany w SIWZ w powyższym zakresie.

1. Zamawiający w dokumencie wzoru umowy, § 11 GWARANCJA, ust. 10.2 pisze „*W przypadku wykrycia przez Zamawiającego Dysfunkcji Zamawiający dokona jego zgłoszenia oraz nada mu kategorię.*”. Wykonawca zwraca uwagę, że nadanie kategorii zgłoszenia należy do strony rejestrującej to zgłoszenie i świadczącej usługę wsparcia. Dlatego Wykonawca wnosi o zmianę tego zapisu na następujący: „*W przypadku wykrycia przez Zamawiającego Dysfunkcji Zamawiający dokona jego zgłoszenia, a Wykonawca nada mu kategorię.*”.

Podobnie w przypadku punktu 4 Procedury Serwisowej (tak jak przytoczony powyżej). W tym punkcie Zamawiający również precyzuje, że to on nadaje kategorię. Wykonawca zwraca uwagę, że Zamawiający może niedostatecznie znać system i uwarunkowania jego działania, przez co nie jest w stanie precyzyjnie określić odpowiedniej kategorii. To leży po stronie Wykonawcy. Wykonawca wnosi o korektę tych dwóch zapisów zgodnie z propozycją Wykonawcy.

Zamawiający nie wyraża zgody na dokonywanie kategoryzacji po stronie Wykonawcy. Wykonawca ma możliwość zmiany kategorii w porozumieniu z Zamawiającym zgodnie z zapisem Załącznika nr 6 do Umowy - Procedura serwisu:

„Procedura przyjęcia Zgłoszenia Serwisowego: pkt. 4. W Zgłoszeniu Serwisowym Zamawiający określa Kategorię Dysfunkcji, a jej zmiana przez Wykonującego wymaga pisemnego (e-mail lub w portalu zgłoszeń) uzasadnienia i możliwa jest jedynie w porozumieniu z pracownikiem Zamawiającego dokonującym zgłoszenia lub jego przełożonym.”.

1. Zamawiający w dokumencie wzoru umowy, § 11 GWARANCJA, ust. 10.3. pisze „*W razie otrzymania przez Wykonawcę zgłoszenia lub w razie uzyskania przez Wykonawcę wiedzy o wystąpieniu Dysfunkcji z innego źródła niż zgłoszenie Zamawiającego Wykonawca zobowiązany będzie do podjęcia działań zmierzających do usunięcia Dysfunkcji. Wykonawca jest zobowiązany do poinformowania Zamawiającego o podjęciu działań w Czasie Reakcji.*”. Wykonawca wnosi o usunięcie tego zapisu. Zdaniem Wykonawcy zapis ten sprowadza się do tego, że Zamawiający nie ma obowiązku używania oficjalnego kanału kontaktowego i może rościć prawa do naprawy nawet takich zgłoszeń, których nie wykonał formalnie, lub których nie wykonał wcale. Jest to zapis wykraczający poza zakres gwarancji i rękojmi.

Zapis dotyczył oprogramowania i w tym zakresie dokonano zminy w Umowie.

Zamawiający przez ten zapis rozumie, powzięcie informacji przez Wykonawcę o występowaniu Dysfunkcji *oprogramowania* np. od innego Klienta, u którego uruchomiona jest ta sama wersja Systemu, i zabezpiecza się w ten sposób, że otrzyma od Wykonawcy aktualną i wolną od wad wersję Systemu nawet jeśli u Zamawiającego dana Dysfunkcja nie wystąpiła.

1. Zamawiający w dokumencie wzoru umowy, § 12 ust. 13 opisuje sytuację, w której Zamawiający nie ma obowiązku instalacji aktualizacji, mimo iż Wykonawca ma prawo do ostrzeżenia Zamawiającego przed skutkiem niedokonania aktualizacji. W związku z tym Wykonawca wnosi o zapis we wzorze umowy: „*Wykonawca nie ponosi odpowiedzialności za błędy wynikające z decyzji Zamawiającego i nie dokonania*

*przez Zamawiającego aktualizacji systemu w przypadku, gdy Zamawiający został poinformowany o konsekwencjach rezygnacji z aktualizacji systemu*”.

Zamawiajacy dopuszcza umieszczenie w Umowie powyższego zapisu.

1. Zamawiający w dokumencie Procedura Serwisu, punkt 11 tabeli opisuje wymaganie zgłaszania i realizowania propozycji zmian w oprogramowaniu. Wykonawca zwraca uwagę, że założenia serwisu w ramach gwarancji dotyczą jedynie naprawy systemu zgodnie z kategoriami zgłoszeń określonymi w tym samym dokumencie. Gwarancja nie obejmuje wykonywania zmian na żądanie Zamawiającego, tzw. propozycji. Dodatkowo Zamawiający precyzuje wąski zakres możliwości odmowy przez Wykonawcę wykonania tego typu prac. Tymczasem Wykonawca w ramach gwarancji w ogóle nie ma obowiązku wykonywać propozycji zmian, Zamawiający nawet nie precyzuje definicji kategorii takiego zgłoszenia. Wykonawca wnosi o usunięcie tych zapisów z dokumentu (a dokładnie całego punktu 11 tabeli), gdyż dokument z założenia i zgodnie z zasadami gwarancji i rękojmi, ma opisywać procedurę serwisową w ramach gwarancji, nie zaś w ramach rozwoju zleconego przez Zamawiającego.

Tak samo w przypadku punktu 15 tabeli, który zakłada wsparcie w planowaniu zmian w systemie. Wykonawca wnosi o usunięcie również punktu 15 tabeli. Jeżeli Zamawiający wymaga w ramach postępowania rozwoju systemu zgodnie z własnymi wymaganiami, które mają na celu modyfikację systemu w zakresie występującym poza Opis Przedmiotu Zamówienia, to Zamawiający powinien wyznaczyć na ten cel dodatkowy budżet do wykorzystania, liczony np. w godzinach, aby dostosować zamawiany system do specyficznych potrzeb. W innym wypadku wskazane zapisy wskazują na nieograniczone pole rozwoju systemu zgodnie z propozycjami Zamawiającego, tymczasem budżet postępowania jest ograniczony i zakłada dostawę systemu zgodnie z wymaganiami oraz jego utrzymanie w ramach gwarancji.

Procedura opisuje Zmiany zawarte w pkt. 5.4 § 12 Umowy. Punkt 15 tabeli „Procedura Serwisu” został wykreślony.

1. Zamawiający w dokumencie Procedury Serwisowej, sekcja Procedura podejmowania Prac Serwisowych wymaga formy pisemnej w przypadku odmowy dostępu do systemu przez Zamawiającego. Wykonawca zwraca uwagę, że znacznie wydłuża to okres naprawy / usunięcia wad opisanych w zgłoszeniu. Wykonawca wnosi o zmianę zapisu dot. formy pisemnej na email (lub inną formę elektroniczną), co znacznie skróci czas oczekiwania na odpowiedź. Propozycja dotyczy całego dokumentu Procedury.

Według Zamawiającego e-mail jest formą pisemną. Dopuszczamy zatem formy pisemne: e-mail, faks lub tradycyjna (papierowa).

1. Zamawiający w dokumencie Procedury Serwisowej, sekcja Warunki zdalnego dostępu Wykonawcy do zasobów Zamawiającego opisuje „*7. Wykonawca zapewni bezpieczny kanał komunikacji VPN i określi numery portów TCP wykorzystywanych w komunikacji.*”. Czy Zamawiający dopuści inne formy połączeń zdalnych, np. TeamViewer lub równoważne? Znacznie ułatwi to połączenia zdalne, a jest równie bezpieczne i wydajne.

TAK, Zamawiający dopuści inne rozwiązania zdalnego dostępu, ale konieczne jest zapewnienie bezpiecznego kanału transmisji bez pośrednika mogącego odszyfrować przesyłane dane.

1. Zamawiający w dokumencie Wzoru umowy (załącznik nr 7 do SIWZ) precyzuje definicję analizy oraz precyzuje przedmiot umowy, w tym „*przeprowadzenie analizy Systemu pod kątem wymagań funkcjonalnych i poza funkcjonalnych oraz zaprojektowania architektury systemu*”. Wykonawca zwraca uwagę, że ww. dokumentacja jest dokumentacją poufną, której nie przekazuje się podmiotom trzecim. Dokumentacja analityczna stanowi know-how dostawcy i nie może być przekazana osobom trzecim w celu uzyskania informacji o architekturze systemu. Dodatkowo etap wykonania analizy lub jej przekazania jest zbędny z punktu widzenia przedmiotu zamówienia, tj. dostawy systemów zgodnie z wyszczególnionymi wymaganiami. Co w przypadku, gdy Wykonawca posiada już produkt, który spełnia wymagania Zamawiającego? Niemożliwe jest wykonanie etapu analizy, gdyż sama dokumentacja analityczna została wykonana już wcześniej, na potrzeby wewnętrzne producenta oprogramowania. Element ten wg Wykonawcy jest zbędny w wykonaniu przedmiotu zamówienia, Wykonawca wnosi o usunięcie zapisów dotyczących sporządzenia i dostawy dokumentacji analitycznej ze względu na ochronę własności intelektualnej Wykonawcy.

Zamawiający zmienił zapisy SIWZ w tym zakresie.

1. Zamawiający w dokumencie Wzoru umowy (załącznik nr 7 do SIWZ), § 5 HARMONOGRAM, ust. 7 Zamawiający pisze „*Jeżeli opóźnienie wynika z okoliczności leżących po stronie Wykonawcy, Wykonawca będzie zobowiązany do wykonywania ewentualnych dodatkowych prac wynikających z opóźnienia, jakie się okażą niezbędne do realizacji Umowy.*”. Wykonawca zwraca uwagę, iż opóźnienie jest terminem odnoszącym się do sytuacji obiektywnej, na którą może mieć wpływ wiele czynników. Dlatego też Wykonawca wnosi o zmianę określenia „opóźnienie” na „zwłokę”, gdyż zwłoka jednoznacznie wskazuje na działanie strony umowy.

Zamawiajacy dopuszcza zmianę wyrażenia „opóźnienie” na „zwłoka” z wyłączeniem par.21 ust 5.p.11

1. Zamawiający w dokumencie Wzoru umowy (załącznik nr 7 do SIWZ), § 21 KARY UMOWNE pisze „*Kary umowne są niezależne od siebie i należą się Zamawiającemu w pełnej wysokości nawet w przypadku, gdy z powodu jednego zdarzenia naliczona jest więcej niż jedna kara.*”. Wykonawca wnosi o zmianę lub usunięcie tego zapisu, ponieważ obciążanie dwukrotnie karą umowną za tę samą okoliczność przejawiającą się w nienależytym wykonaniu zobowiązania uznać należy za sprzeczne z naturą odpowiedzialności odszkodowawczej (art. 353¹ w zw. z art. 361 §1i2 w zw. z art. 483 §1 i 483 §1 KC) (por. wyrok SO w Warszawie z dnia 20 grudnia 2016 r., sygn. akt. XVI GC 190/15).

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

1. Zamawiający w dokumencie Wzoru umowy (załącznik nr 7 do SIWZ), § 21 KARY UMOWNE używa określenia „opóźnienie”, podobnie jak w przypadku § 5 HARMONOGRAM. Wykonawca wnosi o zmianę wszystkich zapisów posiadających zwrot „opóźnienie” na „zwłokę”, ponieważ nie każde opóźnienie musi wynikać z winy Wykonawcy. Zwrot „zwłoka” jasno sugeruje, że jest to opóźnienie z winy jednej ze stron umowy.

Zamawiajacy dopuszcza zmianę wyrażenia „opóźnienie” na „zwłoka” z wyłączeniem par. 21 ust 5 p. 11

1. Zamawiający w dokumencie Opisu Przedmiotu Zamówienia opisuje jeden z zakresów dot. Elektronicznego Obiegu Dokumentów jako „*Dostawa Systemów EOD (z wyłączeniem dostawy EZD PUW) oraz Szyny Danych wraz z zestawem konektorów u każdego z partnerów projektu na poziomie lokalnym. Dostawa portalu Usług elektronicznych oraz Szyny Danych na poziomie centralnym*”. Zamawiający używa tutaj określenia „*z wyłączeniem dostawy EZD PUW*”. Czy Zamawiający przewiduje jednak jakąkolwiek dostawę systemu EOD innego niż „EZD PUW”? Co prawda w rozdziale 7.1 „System EOD (EZD PUW)” Zamawiający pisze „*EZD PUW – pozyskanie i wdrożenie systemu nie jest przedmiotem zamówienia. Zamieszczona dokumentacja interfejsu EZD służy jedynie zdefiniowaniu parametrów i zasad wymiany danych pomiędzy portalem E-usług i systemem EZD PUW.*”. Jednak porównując te zapisy można dojść do wniosku, że istnieją lokalizacje, które wymagają dostawy systemu EOD, jednak brak jest możliwości określenia, w jakim zakresie oraz które to lokalizacje. Wykonawca wnosi o potwierdzenie, że dostawa systemu EOD nie jest wymagana w ramach tego postępowania.

W ramach tego postępowania nie jest wymagane dostarczenie systemu EOD.

1. Zamawiający w Opisie Przedmiotu Zamówienia, rozdział 7, wymaganie WSZL1 opisuje „*Komunikacja pomiędzy SUE a SD: udostępnianie usług SD oraz EOD na potrzeby SUE w JST musi być realizowane przez pośrednią warstwę integracyjną - Szynę Danych.*”. Jako że systemy dziedzinowe nie są przedmiotem zamówienia, a poszczególni Partnerzy mogą używać różnych systemów, to Wykonawca wnosi o potwierdzenie, że w ramach postępowania należy w tym zakresie jedynie dostarczyć SUE i udostępnić usługi do integracji, i po stronie Wykonawcy leży zapewnienie, że producent Systemu Dziedzinowego obecnie używanego u Partnera zintegruje się z udostępnionymi usługami.

Zamawiający następnie w podrozdziale 7.3 opisuje szereg wymagań, w ramach których definiuje, że SD (System Dziedzinowy) musi udostępniać pewne dane w wymaganym zakresie (przykład: „*Każdy SD integrowany z SUE musi udostępniać informacje o kontrahentach w zakresie nie mniejszym niż: Nazwa/Nazwisko, Imię, Pesel, NIP, Adres z uwzględnieniem wskazań na słownik TERYT*” itd.). Wykonawca w tym wypadku również prosi o potwierdzenie, że jest to jedynie informacja o tym, jakiego typu danych Wykonawca ma się spodziewać od strony Systemów Dziedzinowych używanych u Partnerów i to po stronie Wykonawcy leży zapewnienie uzyskania tych danych od autorów Systemów Dziedzinowych.

Zapis znalazł się w SIWZ przez pomyłkę, to postępowanie nie obejmuje swoim zakresem wdrożenia i integracji systemów EOD i SD. Zamawiający wprowadził zmiany w tym zakresie.

1. Podobnie jak wyżej, w Opisie Przedmiotu Zamówienia, podrozdział 7.2 dot. warstwy lokalnej szyny danych, Zamawiający w informacji wstępnej opisuje „*Moduł przeznaczony jest do nadzoru nad integrowanymi danymi na poziomie lokalnym pomiędzy SD a EOD oraz umożliwiający udostępnienie danych z SD oraz EOD na potrzeby SUE centralnego.*”. W tym wypadku Zamawiający ponownie pisze o integracji, która nie ma odzwierciedlenia w wykazie elementów dostawy, mianowicie pisze o szynie danych, która będzie integrować dane „udostępnione z SD oraz EOD na potrzeby SUE centralnego”. Zamawiający sugeruje tym samym, że elementem spełnienia przedmiotu zamówienia będzie również integracja danych pochodzących z bliżej nieokreślonych Systemów Dziedzinowych. Wykonawca rozumie, że prace związane z pozyskaniem danych z Systemów Dziedzinowych leżą po stronie Wykonawcy. Wykonawca prosi o potwierdzenie, że ta interpretacja zapisów jest prawidłowa.

Zapis znalazł się w SIWZ przez pomyłkę, to postępowanie nie obejmuje swoim zakresem wdrożenia i integracji systemów EOD i SD. Zamawiający wprowadził zmiany w tym zakresie.

1. Zamawiający, w dokumencie „Prcedura Serwisu”, sekcja „Procedura podejmowania Prac Serwisowych”, pkt. pisze „*Wykonawca dołoży starań, aby Realizacja Zgłoszenia Serwisowego nastąpiła w możliwie krótkim czasie tak, aby uciążliwość spowodowana istnieniem Dysfunkcji jak najkrócej, nie dłużej jednak niż:*

*4 godziny dla stanu krytycznego,*

*2 dni robocze dla awarii,*

*15 dni roboczych dla błędu,*

*30 dni roboczych dla usterki*

*od momentu dokonania Zgłoszenia Serwisowego.*”.

Wykonawca zwraca uwagę, że czasy realizacji serwisu dla stanu krytycznego oraz awarii są wygórowane i niemożliwe do dotrzymania ze względu na uwarunkowania technologiczne i organizacyjne. Dostarczenie poprawki w przeciągu 4 godzin jest też utrudnione ze względu na dotrzymanie ram okienka serwisowego, dostarczenia poprawki do Partnera projektu itd. W takim wypadku ewentualny Wykonawca ma obowiązek dostarczenia poprawki w przeciągu krótkiego czasu liczonego w godzinach, a Zamawiający ma czas na potwierdzenie poprawki wynoszący 7 dni. Jest to nieproporcjonalne pod kątem prac, jakie ma wykonać Zamawiający i Wykonawca. Wykonawca wnosi, aby czasy na naprawę wynosiły kolejno: dla stanu krytycznego minimum 10 godzin, dla awarii minimum 3 dni.

Słownik pojęć definiuje poziomy Dysfunkcji. Dysfunkcja KRYTYCZNA powoduje zatrzymanie pracy Urzędu spowodowane Dysfunkcją dostarczonego Systemu. Dzięki konieczności stosowania architektury HA Zamawiający minimalizuje wystąpienie takich sytuacji kiedy wymagane będzie sklasyfikowanie Dysfunkcji jako Krytyczna. Niemniej jednak w związku z rodzajem prowadzonej przez partnerów Projektu działalności w przypadku kiedy wystąpi taka sytuacja, której przykładu w chwili obecnej Zamawiający nawet nie jest w stanie wymyślić, Zamawiający musi zabezpieczyć się przed sytuacją kiedy Urząd nie będzie mógł funkcjonować przez cały dzień i nie będzie mógł wypełnić obowiązków, które nakładają na niego różne Ustawy.

1. Zamawiający w dokumencie wzoru umowy, sekcja KARY ZA NIENALEŻYTE WYKONANIE ZOBOWIĄZAŃ GWARANCYJNYCH I USŁUG UTRZYMANIA, pkt. 11 pisze „*Zamawiający naliczy kary umowne za niedochowanie Czasu Naprawy wskazanego w § 11 ust. 7 Umowy:*

*w odniesieniu do Stanu Krytycznego – 200,00 PLN za każdą rozpoczętą godzinę opóźnienia;*

*w odniesieniu do Awarii – 100,00 PLN za każdą rozpoczętą godzinę opóźnienia;*

*w odniesieniu do Błędu – 50,00 PLN za każdy rozpoczęty dzień opóźnienia;*

*W odniesieniu do Usterki – 25,00 PLN za każdy rozpoczęty dzień opóźnienia.*”.

Wykonawca zwraca uwagę, że nie każde opóźnienie musi wynikać z winy Wykonawcy, a wysokość kar w pierwotnym brzmieniu jest rażąco wysoka. Wykonawca wnosi o zmianę wysokości kar umownych ze względu na fakt, że niedochowanie czasu realizacji nie zawsze leży po stronie Zamawiającego, a weryfikacja problemu po stronie zgłaszającego nie zawsze jest możliwa w dogodnym czasie. Wykonawca proponuje obniżenie kar umownych:

w odniesieniu do Stanu Krytycznego – 50,00 PLN za każdą rozpoczętą godzinę opóźnienia;

w odniesieniu do Awarii – 25,00 PLN za każdą rozpoczętą godzinę opóźnienia;

w odniesieniu do Błędu – 10,00 PLN za każdy rozpoczęty dzień opóźnienia;

w odniesieniu do Usterki – 5,00 PLN za każdy rozpoczęty dzień opóźnienia.

Zamawiający zmienił określenie opóźnienie na zwłoka i podtrzymał wysokość kar umownych.

1. § 11 pkt. 15 Załącznika nr 7 do SIWZ – Wzór umowy

Zgodnie § 11 pkt. 15 Załącznika nr 7 do SIWZ – Wzór umowy, Zamawiający nie jest zobowiązany do wydania Systemu lub jego elementu w celu świadczenia usług gwarancyjnych, w rozumieniu przepisów Kodeksu cywilnego o gwarancji.

Powyższe stoi w sprzeczności z następującymi postanowieniami Załącznika nr 7 do SIWZ – Wzór umowy:

Wszystkie naprawy gwarancyjne sprzętu realizowane będą w miejscu instalacji (§ 11 pkt. 11 Załącznika nr 7 do SIWZ – Wzór umowy), a na podstawie § 3 ust. 4 Załącznika nr 7 do SIWZ – Wzór Umowy,

Wykonawca zobowiązuje się dostarczyć Zamawiającemu i przenieść na jego własność sprzęt komputerowy z zainstalowanym oprogramowaniem, zwane łącznie w dalszej części umowy „sprzętem”, o parametrach technicznych wynikających z oferty Wykonawcy i zgodnych z parametrami minimalnymi opisanymi w Szczegółowym Opisie Przedmiotu Zamówienia (Błąd! Nie można odnaleźć źródła odwołania. do Umowy).

W związku z okolicznością, że powyższe postanowienia pozostają ze sobą w sprzeczności, Wykonawca zwraca się z prośbą o zmianę proponowanej treści § 11 pkt. 15 Załącznika nr 7 do SIWZ – Wzór umowy, na następującą:

„Zamawiający jest zobowiązany do wydania Systemu lub jego elementu w celu świadczenia usług gwarancyjnych, w rozumieniu przepisów Kodeksu cywilnego o gwarancji.”

Możliwe będzie wydanie sprzętu z zastrzeżeniem, że u Zamawiajacego pozostają wszystkie nośniki danych [np. dyski twarde komputerów] mogące zawierać dane osobowe lub poufne.

1. §12 ust 5 pkt. 5.3 Załącznika nr 7 do SIWZ – Wzór umowy

Zgodnie z §12 ust 5 pkt. 5.3 Załącznika nr 7 do SIWZ – Wzór umowy: „Usługi Utrzymania obejmują w szczególności: dokonywanie zmian w Oprogramowaniu Dedykowanym, nie wynikających z nieprawidłowego działania Oprogramowania, a wynikających ze zmiany obowiązującego prawa w terminie 30 dni od dnia otrzymania przez Wykonawcę pisemnego zlecenia od Zamawiającego; zmiany w Oprogramowaniu Dedykowanym będą dotyczyły zmian wynikających z obowiązujących przepisów prawnych opublikowanych w Dzienniku Ustaw RP oraz w Dzienniku Urzędowym RP „Monitor Polski”, a także zmian prawa lokalnego i procedur wewnętrznych obowiązujących w jednostce Zamawiającego oraz dotyczyć będą funkcjonalności istniejących i wdrożonych u Zamawiającego zgodnie z Umową.”

W związku z treścią zacytowanego postanowienia, Wykonawca zwraca się z zapytaniem, czy prawidłowym jest takie ukształtowanie systemu utrzymania, zgodnie którym Wykonawca zobowiązany jest dostosowywać Oprogramowanie Dedykowane do procedur wewnętrznych obowiązujących w jednostce Zmawiającego i na które Zamawiający bezpośrednio wpływa?

Procedury wewnętrzne partnerów projektu wynikają z różnych przepisów prawa, niedopuszczalnym jest posiadanie i użytkowanie Systemu niezgodnego z prawem i wynikającymi z niego uregulowaniami wewnętrznymi Zamawiającego i partnerów projektu.

1. §9 ust 2 pkt. 2.1.3. Załącznika nr 7 do SIWZ – Wzór umowy oraz §12 ust 5 pkt. 5.3 Załącznika nr 7 do SIWZ – Wzór umowy

We wskazanych wyżej postanowieniach Wzoru umowy pojawia się pojęcia „prawa lokalnego”. W związku z okolicznością, że wskazane pojęcie nie pojawia się w treści Konstytucji Rzeczpospolitej Polskiej jako źródło prawa powszechnie obowiązującego, ani nie występuje w terminologii przyjętej na gruncie ustaw, Wykonawca zwraca się z prośbą o zastąpienie pojęcia „prawa lokalnego” pojęciem „prawa miejscowego”.

Zamawiający wprowadził zmiany w SIWZ w tym zakresie.

1. §21 ust. 5 - 11 Załącznika nr 7 do SIWZ – Wzór umowy

Zgodnie z §21 ust. 5 Załącznika nr 7 do SIWZ – Wzór umowy: „O ile wyraźnie nie postanowiono inaczej, w zakresie kar umownych opisanych Umową, odpowiedzialność za opóźnienie oznacza przyjęcie przez Wykonawcę odpowiedzialności za przekroczenie terminu wskazanego w Umowie lub wyznaczonego zgodnie z postanowieniami Umowy na zasadzie ryzyka, od której może się uwolnić wyłącznie wykazując, że opóźnienie nastąpiło z przyczyn, za które odpowiedzialność ponosi Zamawiający lub było spowodowane przyczynami o charakterze siły wyższej.”

W tym miejscu należy zwrócić uwagę, że W tym miejscu wskazać należy, że zgodnie z wyrokiem Sądu Najwyższego Izby Cywilnej z dnia 27.09.2013 r., sygn. akt I CSK 748/12: „Rozszerzając na podstawie art. 473 § 1 Kodeksu Cywilnego (dalej: „KC”) odpowiedzialność dłużnika z tytułu kary umownej (art. 483 § 1 KC), strony muszą w umowie wyraźnie określić, za jakie inne - niż wynikające z ustawy - okoliczności dłużnik ma ponosić odpowiedzialność. Nie mogą to być okoliczności obciążające wierzyciela (art. 3531 KC). Choć odpowiedzialność dłużnika z tytułu kary umownej za niewykonanie lub nienależyte wykonanie zobowiązania nie jest uwarunkowana poniesieniem przez wierzyciela szkody, to jest uwarunkowana pozostałymi przesłankami odpowiedzialności kontraktowej przewidzianej w art. 471 KC. Kara umowna stanowi odszkodowanie umowne i przysługuje wierzycielowi jedynie wtedy, gdy niewykonanie lub nienależyte wykonanie umowy jest następstwem okoliczności, za które dłużnik ponosi odpowiedzialność. Innymi słowy zakres odpowiedzialności z tytułu kary umownej pokrywa się z zakresem ogólnej odpowiedzialności kontraktowej dłużnika, który zwolniony jest od obowiązku zapłaty kary, gdy wykaże, że niewykonanie lub nienależyte wykonanie zobowiązania było następstwem okoliczności, za które nie ponosi odpowiedzialności. Oznacza to, że przesłanką dochodzenia zapłaty kary umownej jest wina dłużnika w postaci co najmniej niedbalstwa.”

W świetle przepisów prawa powszechnie obowiązującego oraz orzecznictwa tak sądów powszechnych jak i Sądu Najwyższego - kara umowna może zostać naliczona jedynie za zwłokę tj. kwalifikowaną i zawinioną postać opóźnienia, a nie za opóźnienia za które dłużnik nie ponosi odpowiedzialności. Warunkiem zatem powstania odpowiedzialności dłużnika, która warunkowałaby zasadność nałożenia na niego kar umownych, jest nie tylko wystąpienie po stronie dłużnika szkody oraz związku przyczynowo-skutkowego pomiędzy zaistnieniem szkody a działaniem dłużnika, ale również wina po stronie dłużnika.

W związku z powyższym Wykonawca zwraca się z prośbą o zmianę brzmienia poniżej postanowienia §21 ust. 5 Załącznika nr 7 do SIWZ – Wzór umowy następującym brzmieniem:

O ile wyraźnie nie postanowiono inaczej, w zakresie kar umownych opisanych Umową, odpowiedzialność za zwłokę oznacza przyjęcie przez Wykonawcę odpowiedzialności za przekroczenie terminu wskazanego w Umowie lub wyznaczonego zgodnie z postanowieniami Umowy na zasadzie winy.

Ponadto Wykonawca zwraca się z prośbą o zastąpienie terminu „opóźnienie” w §21 ust. 5 - 11 Załącznika nr 7 do SIWZ – Wzór umowy terminem „zwłoka”.

Zamawiający wprowadził zmiany w SIWZ w tym zakresie.

1. §21 ust. 10 Załącznika nr 7 do SIWZ – Wzór umowy

Biorąc pod uwagę okoliczności wskazane w Pytaniu nr 6, Wykonawca zwraca się z prośbą o zmianę brzmienia poniżej postanowienia §21 ust. 10 Załącznika nr 7 do SIWZ – Wzór umowy następującym brzmieniem:

„Wykonawca ponosi odpowiedzialność za zwłokę w wykonywaniu zobowiązań gwarancyjnych i Usług Utrzymania (Czas Naprawy), przez co należy rozumieć przyjęcie przez Wykonawcę odpowiedzialności na zasadzie winy.”

Zamawiający wprowadził zmiany w SIWZ w tym zakresie.

1. §21 ust. 12 i 13 Załącznika nr 7 do SIWZ – Wzór umowy

Zgodnie z obecnym brzmieniem §21 ust. 12 Załącznika nr 7 do SIWZ – Wzór umowy: „Zamawiający naliczy karę umowną w wysokości 500000,00 PLN w przypadku odstąpienia od Umowy z powodu okoliczności leżących po stronie Wykonawcy. Dla uniknięcia wątpliwości kara jest należna zarówno w przypadku odstąpienia umownego, jak i na podstawie przepisów ustawy, zarówno odstąpienia ze skutkiem do całej Umowy, jak i odstąpienia w części, jeżeli Umowa lub przepis to przewiduje.”

Dalej zgodnie z §21 ust. 13 Załącznika nr 7 do SIWZ – Wzór umowy, Zamawiający naliczy karę umowną w wysokości 500000,00 PLN w przypadku wypowiedzenia Umowy w zakresie Usług Utrzymania z powodu okoliczności leżących po stronie Wykonawcy.

W związku z okolicznością, że powyższe postanowienia pozostają w sprzeczności z przepisami prawa powszechnie obowiązującego (co wyczerpująco omówiono w Pytaniach nr 6 i 7), Wykonawca zwraca się z prośbą o zmianę aktualnego brzmienia wskazanych postanowień i zastąpienie ich następującą treścią:

§21 ust. 12 Załącznika nr 7 do SIWZ – Wzór umowy

 „Zamawiający naliczy karę umowną w wysokości 500000,00 PLN w przypadku odstąpienia od Umowy z powodu okoliczności zawinionych przez Wykonawcę. Dla uniknięcia wątpliwości kara jest należna zarówno w przypadku odstąpienia umownego, jak i na podstawie przepisów ustawy, zarówno odstąpienia ze skutkiem do całej Umowy, jak i odstąpienia w części, jeżeli Umowa lub przepis to przewiduje.”

§21 ust. 13 Załącznika nr 7 do SIWZ – Wzór umowy

Zamawiający naliczy karę umowną w wysokości 500000,00 PLN w przypadku wypowiedzenia Umowy w zakresie Usług Utrzymania z powodu okoliczności zawinionych przez Wykonawcę.

Zamawiający podtrzymuje zapisy w SIWZ w tym zakresie.

1. §21 ust. 16 Załącznika nr 7 do SIWZ – Wzór umowy

Zgodnie z §21 ust. 16 Załącznika nr 7 do SIWZ – Wzoru umowy: „Za każdy przypadek posłużenia się Podwykonawcą, co do którego zachodzą podstawy wykluczenia Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1000,00 zł z zastrzeżeniem, o którym mowa w §7 ust. 11 pkt. 2.”

Jak wskazano w treści pytań 6-8, zgodnie z przepisami prawa powszechnie obowiązującego kary umowne można przewidzieć wyłącznie za okoliczności zawinione przez Wykonawcę. W związku z powyższym

Wykonawca zwraca się z prośbą o zastąpienie dotychczasowego brzmienia postanowienia następującym brzmieniem:

„Za każdy przypadek posłużenia się Podwykonawcą, co do którego zachodzą podstawy wykluczenia Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1000,00 zł, jeśli miał wiedzę o podstawach wykluczenia tego Podwykonawcy, z zastrzeżeniem, o którym mowa w §7 ust. 11 pkt. 2.”

Zamawiający podtrzymuje zapisy w SIWZ w tym zakresie.

1. §21 ust. 17 Załącznika nr 7 do SIWZ – Wzór umowy

W związku z uwagami wskazanymi w treści pytań 6-9, Wykonawca zwraca się z prośbą o zmianę brzmienia postanowień na następujące:

§21 ust. 17 Załącznika nr 7 do SIWZ – Wzór umowy:

„Niezależnie od kar umownych opisanych powyżej, Zamawiający naliczy kary umowne:

pkt. 17.1. w przypadku naruszenia zasad ochrony Informacji Poufnych – w wysokości 10000,00 PLN za każdy przypadek zawinionego przez Wykonawcę naruszenia;

17.2. w przypadku, gdy Wykonawca będzie przetwarzał powierzone dane osobowe niezgodnie z treścią niniejszej Umowy, udostępni je osobie nieupoważnionej lub Generalny Inspektor Ochrony Danych Osobowych stwierdzi, że Wykonawca nie respektuje zasad określonych w Ustawie o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2014, poz. 1182 z późn. zm.), Zamawiający obciąży Wykonawcę karami pieniężnymi lub grzywnami nałożonymi z tego powodu na Zamawiającego, a Wykonawca zobowiązuje się do zapłaty kwoty równej wartości uiszczonych kary lub grzywien, jeżeli jego działanie będzie zawinione,

17.3. każdorazowo za zawinione przez Wykonawcę niezatrudnienie osoby wykonującej na umowę o pracę co najmniej z jednej z czynności wskazanych w §21 Umowy, a polegających na wykonywaniu pracy w sposób określony w Kodeksie Pracy – w wysokości stanowiącej iloczyn kwoty minimalnego wynagrodzenia za pracę ustalonego na podstawie przepisów o minimalnym wynagrodzeniu za pracę, obowiązujących w chwili stwierdzenia przez Zamawiającego niedopełnienia przez Wykonawcę wymogu zatrudnienia oraz liczby miesięcy w okresie realizacji Umowy, w których nie dopełniono przedmiotowego wymogu,

17.4. każdorazowo za zawinione niezapewnienie przez Wykonawcę obowiązku zatrudnienia przez Podwykonawcę osoby wykonującej na umowę o pracę co najmniej z jednej z czynności wskazanych w §21 Umowy, a polegających na wykonywaniu pracy w sposób określony w Kodeksie Pracy – w wysokości stanowiącej iloczyn kwoty minimalnego wynagrodzenia za pracę ustalonego na podstawie przepisów o minimalnym wynagrodzeniu za pracę, obowiązujących w chwili stwierdzenia przez Zamawiającego nie zapewnienia przez Wykonawcę niedopełnienia przez podwykonawcę wymogu zatrudnienia oraz liczby miesięcy w okresie realizacji Umowy, w których nie dopełniono przedmiotowego wymogu,

17.5. za zawinione przez Wykonawcę nieprzedłożenie dokumentu, o którym mowa w §21 ust. 3 Umowy, w wysokości 1000,00 złotych za rozpoczęty dzień zwłoki od dnia upływu terminu wyznaczonego na jego złożenie,

17.6. za zawinione i nieterminowe przedkładanie dokumentów, o których mowa w §21 ust.4, w wysokości 1000,00 złotych za rozpoczęty dzień zwłoki od dnia upływu terminu wyznaczonego na ich złożenie.”

Zamawiający podtrzymuje zapisy w SIWZ w tym zakresie.

1. Dotyczy Załącznika nr 2 do SIWZ, Tabela 1. „Ramowy wykaz dostarczanych rozwiązań do poszczególnych Partnerów Projektu” Zamawiający pisze : „Starostwo Powiatowe w Giżycku - 2 lokalizacje” z wskazaniem ilości dostarczonych komponentów. Dodatkowo w pkt. 6.1.1, Tabela 5 „Wymagania ogólne dot. dostarczonego sprzętu”, kod  WSZL16 Zamawiający pisze: „Serwer AD - Do lokalizacji 5,6,7,8,9,10,11 (do 50 użytkowników) Wykonawca dostarczy po min. dwa serwery fizyczne spełniające wymagania z rozdziału 6.1.3; do lokalizacji 1,2,3,4,12 (od 51-150 użytkowników) Wykonawca dostarczy po min. dwa serwery fizyczne spełniające wymagania z rozdziału 6.1.4”

Natomiast w pkt 2.1 „Zarys rozwiązania” Zamawiający dla lokalizacji 11 napisał:

„Powiat Giżycki – dwie lokalizacje:

·         al. 1 Maja 14, 11-500 Giżycko

·         ul. Generała Józefa Zajączka 2, 11-500 Giżycko”

W związku z powyższym Wykonawca ma wątpliwości co do łącznej ilości lokalizacji i ilości urządzeń jakie należy dostarczyć. Prosimy o wyjaśnieni e czy przedmiotową lokalizację 11 należy traktować jako jedną, połączoną miedzy sobą siecią LAN, czy należy traktować jako dwie odrębne lokalizacje, z całkowicie odrębną infrastrukturą dla każdej z nich?

Siedziba Powiatu Giżyckiego znajduje się w dwóch budynkach, logicznie stanowiących jeden Urząd i jedną sieć lokalną.

Powiat Gizycki należy traktować jako jedną lokalizację z dwoma budynkami połączonymi logicznie jako sieć LAN. Odległość budynków od siebie to ok 500 m.

1. Roz. V ust. 1 pkt 2).II lit. d) siwz - czy wartość 4.000.000 zł dotyczy samego opracowania dokumentacji projektowej lub powdrożeniowej systemu informatycznego, czy też dotyczy danego projektu w całości?;

Zapis dotyczy wartości projektu, nie wartości usługi wytworzenia dokumentacji.

1. Roz. VIII ust. 6 siwz - czy Zamawiający potwierdza, że udzieli wyjaśnień na 6 dni przed terminem składania ofert, a nie na 2 dni, jest to postępowanie powyżej progów unijnych;

Zamawiajacy wprowadził stosowną zmienę, jest to oczywiście omyłka pisarska.

1. Zgodnie z art. 25a ust. 2 w związku z ust. 1 Ustawy Prawo zamówień publicznych, informacje zawarte w składanym wraz z ofertą Jednolitym Europejskim Dokumentem Zamówienia (JEDZ) stanowią wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu z postępowania oraz spełnia warunki udziału w postępowaniu.

W związku z powyższym zwracamy się z zapytaniem, czy Zamawiający uzna za wystarczające na etapie składania ofert - wypełnienie JEDZ w Cz. IV Sek. alfa (Zaznaczenie, że spełnia warunki udziału w postępowaniu).

Zamawiający wymaga wypełnienia całego załącznika zgodnie z zamieszczonym formularzem.

1. Dotyczy wzoru umowy - załącznik nr 7, §8- czy Zamawiający wyraża zgodę na dodanie w §8 zdania „Zamawiający będzie chronił udostępnione dane osobowe pracowników Wykonawcy zgodnie z zapisami Ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych”

Zamawiający wyraża zgodę na dodanie w/w pkt. do Umowy.

1. § 23 ust. 15.2 - Wykonawca prosi o doprecyzowania zapisów tj. w sytuacji kontroli inspektorów z Biura GIODO w aspekcie powierzonych danych osobowych przez Zamawiającego.

Zamawiający zgodnie z zapisem SIWZ wymaga poinformowania o wystąpieniu takiej kontroli u Wykonawcy.

1. § 23 ust. 15.5 - Wykonawca wnosi doprecyzowania zapisów tj. w sytuacji incydentu związanego z powierzonymi przez Zamawiającego danymi osobowymi.

Szczegółowe wyjaśnienie pojęcia „incydentu” można odnaleźć w normie PN-ISO/ IEC 27001. Zgodnie z jej treścią przez incydent związany z bezpieczeństwem informacji należy rozumieć pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

1. § 24 - prosimy o zmianę zwrotu informacje poufne na informacje stanowiące tajemnicę przedsiębiorstwa.

Ze względu na charakter Zamawiajacego i dane przez niego przetwarzane, zapis pozostaje nie zmieniony.

1. § 24 - prosimy o sprecyzowanie jak długo po wygaśnięciu/rozwiązaniu umowy Wykonawca jest zobowiązany zachować w tajemnicy pozyskane informacje?

Zgodnie z obowiązującymi w tym zakresie przepisami prawa.

1. Czy w §25 Zamawiający zobowiąże się do ochrony przekazanych danych osobowych pracowników Wykonawcy zgodnie z zapisami Ustawy z 27siewrpnia 1997 r. o ochronie danych osobowych?

Tak, Zamawiający zobowiązuje się do zachowania zapisów Ustawy o ochronie danych osobowych w odniesieniu do pracowników Wykonawcy.

1. Czy Zamawiający wymaga objęcia monitoringiem punktów dostępowych sieci bezprzewodowej?

Zamawiający nie wymaga objęcia monitoringiem punktów dostępowych.

PAKIET 5

1. W szczegółowym Opisie Przedmiotu Zamówienia pkt. 6.1.5 "Wymagania minimalne dotyczące macierzy dyskowej w zasobach lokalnych" Tabela 9 Lp. 2 "Kontrolery dyskowe" Zamawiający oczekuje, że dostarczona macierz dyskowa będzie wyposażona w minimum 2 kontrolery pracujące w trybie active/active z możliwością rozbudowy do 8 kontrolerów dyskowych tworzących jedną logiczną macierz, jednocześnie w Lp. 3 "Wymagana przestrzeń" oczekuje dostarczenia 9 dysków o pojemności nie mniejszej niż 1,2 TB SAS 10 RPM lub szybszych, np. SSD, a w Lp. 4 "Możliwość rozbudowy macierzy" rozbudowy oferowanej macierzy do co najmniej 500 napędów dyskowych, bez wymiany kontrolerów macierzowych, zaś w Lp. 5 "Pamięć cache" minimum 16 GB pamięci cache na każdy kontroler z możliwością rozbudowy do 128 GB. Parametr skalowalności macierzy opisany w Lp. 2 wskazuje na wysokodostępne, skalowalne i drogie macierze klasy Enterprise, natomiast parametry opisane w Lp. 3, 4 i 5 wskazują na skalowalną i wysokodostępną macierz klasy midrange. W celu zaproponowania rozwiązania wydajnego, skalowalnego i ekonomicznie dopasowanego do pozostałych punktów charakteryzujących macierz czy Zamawiający dopuści macierz dyskową, która będzie umożliwiała rozbudowę do 4 kontrolerów dyskowych (wymóg w Lp. 2) przy jednoczesnym spełnieniu pozostałych parametrów opisanych w Lp. 3, 4 i 5?

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

2. W szczegółowym Opisie Przedmiotu Zamówienia pkt. 6.1.5 "Wymagania minimalne dotyczące macierzy dyskowej w zasobach lokalnych" Tabela 9 Lp. 7 "Dostępne interfejsy" Zamawiający oczekuje dostarczenia razem z kontrolerami  minimum 8 interfejsów 1 Gb/s ETH i 8 interfejsów 10Gb/s FC/iSCSI do podłączenia sieci SAN. W związku z faktem, że interfejsy FC nie występują w prędkości 10 Gb/s, a interfejsy Ethernet 10 Gb/s są kompatybilne w dół z 1 Gb/s to czy Zamawiający dopuści macierz wyposażoną w 2x 1 Gb/s ETH, 4x 16 Gb/s FC, 4x 10 Gb/s iSCSI oraz 4x 10 Gb/s ETH (razem osiem interfejsów 10 Gb/s) z możliwością rozbudowy o kolejne 8x 16 Gb/s FC lub 4x 10 Gb/s ETH i 4x 10 Gb/s iSCSI (razem osiem interfejsów 10 Gb/s)?

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

3. Czy Zamawiający dopuści wycenę wsparcia producenta zgodną z godzinami pracy producenta

Zamawiający wymaga wsparcie w godzinach pracy ZAMAWIAJĄCEGO.

6.1.2 Wymagania minimalne dotyczqce routera CE

4. Dot. pkt. 2 - Podstawowe wymaganie sprzętowe  - 2

Czy Zamawiający dopuści urządzenie wyposażone w 1 GB pamięci FLASH?

Zamawiający zmienił zapis SIWZ, z 2GB Flash, na 1 GB Flash.

5. Dot. pkt. 7 - Architektura - 3

Czy Zamawiający dopuści urządzenie bez sprzętowego modułu akceleracji szyfrowania DES/3DES/AES? Funkcjonalność akceleracji szyfrowania będzie realizowana software’owo.

Zamawiający wymaga sprzętowego modułu akceleracji szyfrowania danych.

6. Dot. pkt. 9 - Architektura - 5

Czy Zamawiającemu chodziło o możliwość obsadzenia o moduł z portami FXO zamiast portów FX? Czy Zamawiający dopuści rozwiązanie z możliwością rozbudowy o dodatkowe moduły do maksymalnej liczby 16 portów FXS oraz 4 portów FXO?

Zamawiający dopuści powyższe rozwiązanie.

7. Dot. pkt. 10 - Architektura- 6

Czy Zamawiający dopuści moduł MSR G2 o gęstości nie mniejszej niż 128 kanałów zamiast modułu DSP? Prośba o doprecyzowanie czego Zamawiający oczekuje od modułu przeznaczonego do obsługi Voice’a.

Zamawiający dopuszcza zastosowanie modułów MSR G2 o gęstości co najmniej 128 kanałów. Slot urządzenia przewidziany pod rozbudowę o moduł DSP lub moduł MSR G2 musi mieć możliwość obsadzenia modułem o gęstości nie mniejszej niż 128 kanałów.

Zamawiający wymaga MOŻLIWOŚCI rozbudowy o moduł DSP w przyszłości bez precyzowania jego funkcji, które w momencie ewentualnego zakupu modułów mogą oferować inne niż obecnie dostępne usługi.

1. Czy Zamawiający dopuści rozwiązanie bez możliwości rozbudowy o funkcjonalność kontrolera WLAN?

Zamawiający wymaga możliwości rozbudowy o kontroler WLAN.

9. Dot. pkt. 19- Oprogramowanie- funkcjonalnosc

Czy Zamawiający dopuści urządzenie bez funkcjonalności POLICY BASED ROUTING?

Zamawiający podtrzymuje zapisy w SIWZ w tym zakresie.

10. Dot. pkt. 36 - Zarzqdzanie i konfiguracja

Czy Zamawiający dopuści urządzenie bez możliwości zarządzania za pomocą GUI?

Zamawiający nie zezwala na zastosowanie urządzeń bez GUI.

6.1.7 Wymagania minimalne dotyczqce przelqcznik6w sieciowych

11. Dot. pkt. 26

Czy Zamawiający dopuści urządzenie z równoważnym mechanizmem do badania jakości połączeń zamiast mechanizmu IP SLA?

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

12. W wymaganiach od WD15 do WD 26 Zamawiający pisze, że „Każdy SD integrowany z SUE musi udostępniać informacje”, ale Wykonawca jest odpowiedzialny jedynie za stworzenie konektorów pomiędzy SD, a szyną danych i nie ma wpływu na to jakie dane udostępnia SD. Zatem prosimy o potwierdzenie, że to Zmawiający odpowiada za to jakie dane udostępniają SD i EZD PUW?

Zamawiający zmienił zapisy w tym zakresie wykreślając zbędne zapisy.

To postępowanie nie obejmuje swoim zakresem wdrożenia i integracji systemów EOD i SD.

13. Zamawiający w punkcie 7.4 i 9.8 wymaga „Wykonawca musi działać w oparciu o system zarządzania jakością zgodny z wymaganiami ISO 9001 wydany przez jednostkę akredytowaną w zakresie projektowania, wdrażania i utrzymywania oprogramowania wspomagającego pracę jednostek administracji publicznej lub równoważny oraz w oparciu o system zarządzania jakością zgodny z wymaganiami ISO/IEC 27001 wydany przez jednostkę akredytowaną w zakresie projektowania, wdrażania i utrzymywania oprogramowania wspomagającego pracę jednostek administracji publicznej lub równoważny.”

Prosimy o potwierdzenie zgodnie z interpretacją Wykonwcy, ze  nie jest wymagane od wykonwcy posiadnie certyfikatu ISO.

Zamawiający wymaga aby Wykonawca działał w oparciu o certyfikat ISO, jedynym sposobem potwierdzenia tego jest posiadanie przez Wykonawcę certyfikatu ISO.

14. W ramach wymagania WW3 Zamawiający pisze, że „W ramach usług wdrożeniowych, Wykonawca zrealizuje:

* Udostępnienie na infrastrukturze sprzętowej Partnera systemu EZD oraz Lokalnej Szyny Danych na potrzeby procesu wdrożenia i szkolenia

Ale zgodnie z punktem 7.1 pozyskanie i wdrożenie EZD PUW nie jest przedmiotem Zamówienia zatem jak należy rozumieć ten zapis?

Zamawiający wymaga udostępnienia maszyny wirtualnej na potrzeby instalacji EZD PUW i zestawu konektorów.

PAKIET 6

1. Zamawiający w par. 5 ust. 3 wzoru umowy wymaga, aby Wykonawca w terminie 5 dni od podpisania umowy przedstawił harmonogram ramowy określający zakres dostaw i usług. Wykonawca zwraca uwagę, że biorąc pod uwagę bardzo obszerny zakres przedmiotu zamówienia termin ten jest stanowczo zbyt krótki. Prosimy o zmianę tego terminu na 21 dni od dnia podpisania umowy.

Zamawiajacy zmienił zapis na 21 dni roboczych.

2. Zamawiający w par. 12 ust. 14 pkt 14.1.2 wzoru mowy zastrzega możliwość wypowiedzenia umowy, gdy w miesiącu kalendarzowym Czas Naprawy Błędu Krytycznego nie został dochowany więcej niż trzy razy. Biorąc po uwagę bardzo obszerny przedmiot zamówienia prosimy o zmianę krotności z trzech na więcej niż pięć razy.

Zamawiający nie dopuszcza zmiany w tym zakresie.

3. Zamawiający w par. 21 ust. 11 wzoru umowy nakłada na Wykonawcę karę umowną za niedotrzymanie Czasu Naprawy odwołując się do par. 11 ust. 7. Zwracamy uwagę, że jest to niewłaściwe odniesieni, gdyż par. 11 ust. 7 odnosi się do dysfunkcji poza systemem. Prosimy o zmianę i odwołanie się do właściwego paragrafu umowy.

Zamawiający wprowadził stosowne zmiany w Umowie.

4. Zamawiający w par. 25 ust. 5 wzoru umowy przewiduje nałożenie kary umownej za niezatrudnienie osób na umowę o pracę odwołując się do par. 22. Wykonawca zwraca uwagę, że par. 22 dotyczy podstaw do odstąpienia od umowy a nie wartości naliczanych kar umownych. Prosimy zatem o zmianę zapisu paragrafu i odwołanie się do właściwego zapisu umowy.

Zamawiający wprowadził stosowne zmiany w Umowie. Zapis powienin odnosić się do par. 21.

5. Zamawiający w par. 19 ust. 8 wzoru umowy określił termin płatności na 30 dni od otrzymania faktury VAT przez Zamawiającego. Określenie takiego terminu przez Zamawiającego powoduje, iż Wykonawca będzie zmuszony odprowadzić należny podatek zgodnie z art. 19a ust. 5 pkt. 4) lit. b ustawy z dnia 11.03.2004 r. o podatku od towarów i usług (Dz.U. Nr 54 poz.535 z późn.zm.) od dnia wystawienia faktury VAT. Wobec czego dłuższy termin płatności powoduje, że Wykonawca będzie zmuszony odprowadzić należny podatek jeszcze przed faktycznym uregulowaniem zobowiązania wynikającego z faktury przez Zamawiającego. Dodatkowo Wykonawca informuje, że taki sposób fakturowania wymusza na Wykonawcy wliczenie do projektu dodatkowych kosztów odmiennego fakturowania, co może podrożyć koszt całościowy projektu. Dla Wykonawcy standardowy sposób wystawiania faktur generuje termin płatności liczony od dnia wystawienia faktury VAT. Czy w związku z powyższym Zamawiający wyrazi zgodę na zmianę terminu płatności faktur liczonego od dnia wystawienia faktury w terminie 30 dni, z zastrzeżeniem, że faktura nie może wpłynąć do Zamawiającego później niż w przeciągu 14 dni od daty jej wystawienia?

Zamawiający wyrazi zgodę na powyższy zapis, z zastrzeżeniem, że podstawą do wystawienia faktury przez Wykonawcę jest podpisany przez obie strony protokół odbioru.

6. Zgodnie z § 19 ust. 11 wzoru Umowy, za termin zapłaty wynagrodzenia należnego Wykonawcy uważa się dzień obciążenia rachunku Zamawiającego. Należy zwrócić uwagę, że postanowienie to w obecnym brzmieniu jest niezgodne z powszechną zasadą oraz linią orzecznictwa Sądu Najwyższego (por. uchwała SN z dn. 4 stycznia 1995 r. sygn. CZP 164/94), w myśl których za dzień spełnienia świadczenia pieniężnego w postaci bezgotówkowej uważa się dzień uznania rachunku bankowego wierzyciela (tu Wykonawcy), a nie dzień obciążenia rachunku bankowego dłużnika (tu Zamawiającego). Czy w związku z powyższym Zamawiający wyrazi zgodę na zmianę powyższego zapisu i uzna dniem zapłaty dzień uznania rachunku bankowego Wykonawcy?

Zamawiający nie dopuszcza zmiany w tym zakresie.

7. Zamawiający w par. 21 ust. 2 wzoru umowy zastrzega możliwość naliczania więcej niż jednej kary umownej za jedno przewinienie. W umowie zastrzec można kilka kar umownych (w razie zaistnienia różnych przejawów niewykonania lub nienależytego wykonania zobowiązania) i zsumować je w razie zaistnienia podstaw do naliczenia kilku lub wszystkich z nich. Jednakże nie można stosować i sumować kilku kar za jedno przewinienie. W związku z powyższym wnosimy o usunięcie wskazanego zapisu z wzoru umowy.

Zamawiający nie dopuszcza zmiany w tym zakresie.

8. Zamawiający w par. 21 ust. 4 wzoru umowy zastrzega możliwość potrącenia kar umownych. Wykonawca zwraca uwagę, iż kary umowne winny być dochodzone po uprzednio przeprowadzonym procesie reklamacyjnym. Natomiast nieprawidłowości dotyczące płatności zawsze są regulowane fakturami korygującymi lub też notami księgowymi po rozpatrzeniu złożonej reklamacji. Czy Zamawiający wyraża zgodę na zmianę umowy poprzez dodanie zapisu o tym, że kary umowne będą naliczane po zakończeniu procedury reklamacyjnej, poprzez wystawianie not księgowych lub faktur korygujących?

Zamawiający nie dopuszcza zmiany w tym zakresie.

9. Zamawiający w par. 21 ust. 6, 8 i 9 wzoru umowy nakłada na Wykonawcę kary umowne za opóźnienia w Odbiorach w wysokości 500 zł za każdy rozpoczęty dzień. W ocenie Wykonawcy kary te są zbyt wygórowane. Czy Zamawiający zmieni ich wysokość do 100 zł za każdy dzień?

Zamawiający nie dopuszcza zmiany w tym zakresie.

10. Zamawiający w par. 21 ust. 11 wzoru umowy nakłada na Wykonawcę kary umowne za niedochowanie czasów Naprawy wskazane w pkt 11.1 – 11.4. W naszej ocenie kary te są rażąco wygórowane. Prosimy o zmniejszenie każdej z nich o połowę wartości.

Zamawiający nie dopuszcza zmiany w tym zakresie.

11. Zamawiający w par. 21 ust. 12 i 13 wzoru umowny nakłada na Wykonawcę kary umowne za ewentualne odstąpienie od umowy o wartości 500 000,00 zł. W ocenie Wykonawcy kary te są również zbyt wygórowane. Zamawiający nie powinien wykorzystywać swojej dominującej pozycji ustalając tak wygórowaną wysokość kar umownych. Kary umowne powinny mieć charakter dyscyplinujący w stosunku do Wykonawcy, a nie prowadzić do wzbogacenia się Zamawiającego, a taką funkcję zaczynają pełnić w momencie, gdy okazuje się, iż wartość kary umownej może przekroczyć wartość zapłaty należną Wykonawcy za świadczone usługi. Dodatkowo tak rażąco wygórowane kary można podważyć na drodze sądowej. Zgodnie bowiem z treścią art. 484 § 2K.C. „Jeżeli zobowiązanie zostało w znacznej części wykonane, dłużnik może żądać zmniejszenia kary umownej; to samo dotyczy wypadku, gdy kara umowna jest wygórowana”. Biorąc powyższe pod uwagę wnosimy o zmniejszenie kar do wartości 50 000,00 zł.

Zamawiający nie dopuszcza zmiany w tym zakresie.

12. Zamawiający w par. 21 ust. 14 i 15 wzoru umowy nakłada na Wykonawcę kary umowne za niedotrzymanie postanowień dotyczących zmiany podwykonawcy w wysokości 100 zł za każdy dzień zwłoki. W ocenie Wykonawcy kary te są również zbyt wysokie. Prosimy o zmianę ich wartości do 50 zł za każdy dzień zwłoki.

Zamawiający nie dopuszcza zmiany w tym zakresie.

13. Zamawiający w par. 21 ust. 17.5 i 17.6 wzoru umowy odwołuje się do par. 21 ust. 3 i 4, które nie dotyczą przedkładania dokumentów zatrudnienia na umowę o pracę. Prosimy zatem o poprawę zapisów i odwołanie się do właściwego paragrafu wzoru umowy.

Zamawiający wprowadził zmiany do SIWZ w tym zakresie.

Poprawiony zapis w Umowie odnosi się do par 25. ust.3 i ust.4

14. Zamawiający w par. 21 ust. 17.5 i 17.6 wzoru umowy nakłada na Wykonawcę kary umowne za nieprzedłożenie lub nieterminowe przedłożenie dokumentów o zatrudnieniu osób na umowę o pracę w wysokości 1000 zł za każdy dzień zwłoki. W naszej ocenie kary te są zbyt wygórowane. Prosimy o ich zmniejszenie do wartości 400 zł.

Zamawiający nie dopuszcza zmiany w tym zakresie.

15. Zamawiający nakłada na Wykonawcę szereg kar umownych. Wykonawca przystępując do realizacji zamówienia musi ponieść pewne koszty a projekt powinien być także rentowny. Wykonawca chcąc zabezpieczyć swój zysk na realizacji projektu musi mieć możliwość ograniczenia kar umownych do pewnej wysokości. Czy w związku z powyższym Zamawiający dopuści, aby wysokość naliczonych kar umownych w trakcie realizacji zamówienia nie przekroczyła wysokości 30% całkowitej wartości zamówienia.

Zamawiający nie dopuszcza zmiany w tym zakresie.

16. Zamawiający w par. 21 ust. 12 wzoru umowy zastrzega możliwość naliczenia kary umownej z tytułu odstąpienia od umowy. Prosimy o potwierdzenie, że w przypadku odstąpienia od umowy zostanie naliczona jedynie kara za odstąpienie. Zwracamy uwagę, że po odstąpieniu od umowy wyłączona jest możliwość kumulatywnego dochodzenia kary umownej za odstąpienie i kar zastrzeżonych na wypadek nienależytego wykonania umowy. Uchwała SN z 18.07.2012 r. (III CZP 39/12) przesądziła, że odstępującemu nie przysługuje roszczenie o zapłatę kary umownej na wypadek zwłoki lub opóźnienia, jeżeli w umowie zastrzeżono również taką karę w związku z odstąpieniem od umowy.

Zamawiający nie dopuszcza zmiany w tym zakresie.

17. Zamawiający w Opisie Przedmiotu Zamówienia WD12 w Tabeli 29 ppkt 2 str. 63 zastrzega, aby Wykonawca świadczył usługę transmisji danych w oparciu o sieć IP/MPLS Wykonawcy na bazie własnych łączy. Zapis taki ogranicza konkurencję w niniejszym postępowaniu. Prosimy zatem o usunięcie takiego wymogu z SIWZ.

Zamawiający wprowadził zmiany w SIWZ w tym zakresie.

18. Zamawiający w Opisie Przedmiotu Zamówienia WD13 w Tabeli 29 str. 63 wymaga, aby Wykonawca posiadał co najmniej 5-letnie doświadczenie w prowadzeniu centrum monitoringu i obsługi incydentów (SOC) na polskim rynku~~.~~ Wykonawca takim zapisem ogranicza konkurencyjność niniejszego postępowania. Prosimy zatem o usunięcie wskazanego wymogu z treści pkt 9.6 załącznika 2 do SIWZ (SOPZ D13 w tabeli).

Zamawiający wprowadził zmiany w SIWZ w tym zakresie.

19. Biorąc pod uwagę ilość wątpliwości związanych z przedmiotem zamówienia oraz obszernością zamówienia wnosimy o zmianę terminu składania ofert na 20.12.2017r.

Zamawiający wydłużył termin składania ofert do 04.12.2017 r.

20. Zał.2 – OPZ Str 63 WD8 pkt. II lokalizacje terenowe mają być włączone w postaci CE-2PE oraz WD12 pkt 9. Czy Zamawiający dopuszcza realizację dla lokalizacji terenowych także w postaci 2CE – 2PE, co eliminuje pojedynczy punkt awarii i zwiększa bezpieczeństwo, w postaci jednego routera CE z pojedynczym zasilaczem?

Zamawiający wymaga minimalnej infrastruktury CE-2PE, infrastruktura w postaci 2CE-2PE oferuje parametry lepsze niż minimalne, z zastrzeżeniem utrzymania parametrów minimalnych routera CE.

21. Dodatkowo, czy powyższy zapis oznacza, że CE musi być wyposażone w slot na karty SIM i mieć wbudowany modem LTE, czy dopuszcza się instalację zewnętrznego modemu USB włączonego np. po interfejsie USB do routera?

Zamawiający nie dopuszcza instalacji modemu USB do routera, wymaga zastosowania wbudowanego modemu LTE/3G.

22. Czy Zamawiający dopuszcza włączenie łącza podstawowego z medium światłowodowego do tzw. media konwertera lub modemu optycznego, a następnie do routera poprzez technologię Ethernet kablem miedzianym?

Zamawiający nie dopuszcza takiego rozwiązania.

23. Zamawiający nie specyfikuje przepustowości łącza zapasowego, dopuszczając także łącza radiowe w technologii LTE, działające w oparciu o sieci komórkowe operatorów GSM. Prosimy o doprecyzowanie, czy łącze backupowe może być to łącze z zastosowaniem technologii LTE, a Wykonawca nie jest zobowiązany do zapewnienia poziomu minimalnego przepustowości pasma zachowując technologie LTE.

Z uwagi na możliwość wykorzystania sieci GSM operatora nie będącego Wykonawcą, Wykonawca ma za zadanie dostarczyć i utrzymać łącze zapasowe bez gwarancji prędkości.

24. Łącze zapasowe, Zamawiający raz WD12 pkt 8 dopuszcza jedynie kablowe medium, a innym razem w WD12 pkt 9 dopuszcza się realizację po LTE. Prosimy o doprecyzowanie ostatecznie, czy LTE może być zastosowane jako łącze backupowe?

Zamawiający dopuszcza zastosowanie w jednostkach partnerów projektu łączy 3G/LTE jako łącza backupowe.

25. Zamawiający specyfikuje łącza zapasowe (w OPZ WD12 pkt 9), dopuszcza technologie LTE, inny razem (WD12 pkt. 10) nie dopuszczone są zasoby sieci publicznej Internet. Czy Zamawiający dopuszcza realizację backupu poprzez łącze LTE z zastosowaniem szyfrowanego kanału VPN ?

Zamawiający dopuszcza takie rozwiązanie.

26. Zamawiający specyfikuje iż łącza IP/MPLS muszą być na bazie własnych łączy dostępowych Wykonawcy. Czy w związku z tym, Zamawiający podtrzymuje także zapis w przypadku łącza zapasowego, czy dopuszcza zastosowanie najodpowiedniejszego dla danej lokalizacji łącza od operatora GSM, które pozwoli na określenie, dla danej lokalizacji serwerowni, odpowiedniego łącza zapasowego posiadającego najlepsze parametry łącza. Podtrzymanie zapisu własnych łączy wykluczy jakąkolwiek konkurencyjność w tej dziedzinie i umożliwi złożenie oferty tylko operatorom posiadającym własne usługi GSM/LTE.

Zamawiający wprowadził zmiany w SIWZ w tym zakresie.

27. Wykonawca zwraca uwagę na specyfikację pkt 6.1.2 routera z trzema interfejsami USB, 3xUSB znacznie ogranicza możliwość doboru rozwiązania i wskazuje na platformę jednego z dostawców. Prosimy o zmianę tego zapisu do co najwyżej 2xUSB lub jeden port USB. W przypadku podłączania większej ilości pamięci USB Zamawiający może użyć huba USB.

Zamawiający wprowadził zmiany w SIWZ w tym zakresie.

28. Zawarte w specyfikacji zapisy, dotyczące wymagań urządzeń np. serwery macierze, a także routera, nie mają potwierdzenia w ilości zapotrzebowania, np. na porty, moduły, sloty, funkcjonalność firewall. Dodatkowo, dobór i określenie przez Zamawiającego ilości tych zapotrzebowań jednoznacznie wskazują platformę jednego z dostawców mogącą spełnić te wymogi. Powoduje to, że Wykonawcy nie są traktowani równorzędnie, a tak rozpisane wymagania zwiększają nakład kosztów rozwiązania. Prosimy o usunięcie zapisów nadmiarowych i skupienie się na funkcjach rzeczywiście uzasadnionych. Wykonawcy powinni być równo traktowani oraz mieli możliwość dostarczenia urządzeń adekwatnych pod względem utrzymania ich utrzymania etc., z dodatkowym uwzględnieniem tylko niezbędnych wymogów. Prosimy o wskazanie dokładnego urządzenia spełniającego jednocześnie wszystkie te wymagania. Takich dostępnych urządzeń powinno być wskazane więcej niż jeden, od różnych producentów, np. wiodących w tej dziedzinie Cisco, Juniper, Fortigate etc.

Zgodnie z Art. 38. Ustawy Pzp, ust. 1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia.

Powyższy zapis nie jest pytaniem do treść SIWZ.

29. Prosimy o wyjaśnienie zapotrzebowania na funkcjonalność firewalla w 12 lokalizacjach terenowych zważając na fakt, iż dostęp do Internetu i ochrona firewall opisana jest w części cloud zaplanowanego rozwiązania. Czy tego typu funkcjonalność jest przy takiej architekturze niezbędna?

Funkcjonalność firewalla ma służyć ochronie przed niebezpieczeństwami z wewnątrz sieci.

30. Zamawiający opisuję rozbudowę sieci LAN o punkty PEL, prosimy o doprecyzowanie czy Wykonawca powinien użyci okablowania kategorii 5E?

Wszystkie elementy sieci muszą spełniać wymagania min. Cat. 5E

31. Zamawiający opisuję rozbudowę sieci LAN o punkty PEL, czyli także o gniazda 230V nie na wszystkich planach rozrysowane są tablice rozdzielcze zasilania 230V. W związku z tym, prosimy o uzupełnienie, czy zamawiający posiada plany z wymiarami pomieszczeń w celu oszacowania także długości i przekroju kabli zasilających?

Tak - posiada. Uzupełniono w załącznikach.

32. Zamawiający wskazuje, że Wykonawca musi posiada co najmniej 5 letnie doświadczenie w prowadzeniu COS na polskim rynku. Czy Zamawiający dopuszcza zmniejszenie doświadczenia do 2 lat i rozszerzenia go o rynki Unii Europejskiej?

Zamawiający zmienił zapisy SIWZ w tym zakresie.

33. W punkcie 9.6 Tabela 29, nr WD13, Zamawiający wymaga archiwizacji kopii zapasowych na nośniki taśmowe. W tekście zapytania pojawia się sformułowanie „ Pod pojęciem archiwizacji rozumie się backup z długim czasem retencji”. Prosimy o doprecyzowanie długiego czasu retencji.

Wykonawca w porozumieniu z Zamawiającym w ramach Projektu zobowiązany jest do stworzenia Polityki Backupu, w której określi ten czas na podstawie realnych potrzeb, zastosowanych rozwiązań technicznych w dostarczanym rozwiązaniu minimalizując średni koszt przechowywania kopii w jak najdłuższym terminie.

34. Zamawiający, w tym samym punkcie wymaga aby nośniki taśmowe były przechowywane w innym miejscu niż realizowane kopie zapasowe. Co Zamawiający rozumie pod pojęciem inne miejsce?

Inne miejsce to przynajmniej inny budynek niż ten, w którym wykonywane są kopie.

PAKIET 7

1. W rozdziale nr. 5 „Wymagania ogólne dotyczące dostarczanego rozwiązania”

W tabeli „WP 17” Dla dostarczonego oprogramowania należy dostarczyć: bezterminowe licencje użytkowe oraz subskrypcyjne, okresowe [np. na aktualizację sygnatur wirusów] na min. okres trwałości projektu, tj. 60 msc; nośniki instalacyjne”

Proszę o określnie czy powyższy wymóg definiuje, konieczność dostarczenia nowego aktualnego oprogramowania w przypadku premiery kolejnej wersji o przykładowych nazwach np. Windows Serwer 2020, Windows 11 Pro , Office 2019 ….

- Windows Serwer

- Windows 10 Pro

- Office H&B 2016

Aktualizacja oprogramowania do zawsze najnowszej wersji w czasie trwania projektu ponosi za sobą znaczne koszty .

Zamawiający wymaga jedynie dostarczenia licencji na okres trwałości projektu dla tych produktów, dla których występuje subskrypcyjny model licencjonowania, np. subskrypcja sygnatur antywirusa.

2. Prosimy o uściślenie ilości drukarek wymaganych do realizacji projektu, opisanych w

” 6.1.6.5 Wymagania dotyczące drukarki etykiet”

Po jednej drukarce do każdej JST. Razem 12 szt.

3. Zamawiający w „ 6.1.2 Wymagania minimalne dotyczące routera CE” Opisał urządzenie modularne bez określenia wymogów gwarantujących redundancję rozwiązania co w przypadku awarii w/w urządzenie przy określonym poziomie gwarancji „Wymiana uszkodzonego elementu w trybie min. 8x5xNBD” grozi zatrzymaniem pracy JST.

Obecnie wyspecyfikowany wymóg „Urządzenie musi posiadać funkcjonalność firewalla” nie definiuje poziomu ochrony jaką ma gwarantować funkcjonalność firewall.

W przypadku konieczności korzystania z łącza zapasowego opisanego jako 3g/LTE.

Które to nie gwarantuje działania za każdym razem przez jednego operatora oraz przy 3g nie realizuje funkcjonalności MPLS gwarantującej ochronę zdefiniowaną miedzy innymi w

” VI. System ochrony serwerów w JST” realizowaną przez centralny firewall .

Wyspecyfikowany „Router CE” ze względy na modularną budowę może być rozbudowany przy użyciu modułów jednego producenta co ogranicza konkurencyjność rozwiązania w przyszłej możliwej rozbudowie.

Dla tego zwracamy się z pytaniem czy Zamawiający zgodzi się na zastosowanie w miejsce „Rutera CE” rozwiązania opartego na klastrze urządzeń active-passive, zabezpieczających brzeg sieci i zapewniający redundancję oraz pełną ochronę firewall „next generation firewall” z możliwością dołączenia kolejnych modułów, realizowane za pomocą urządzeń pracujących jako jedno urządzenie o wspólnej wysokości nie większej jak 2U, z możliwością podłączenia bezpośrednio do łączy światłowodowych operatora, spełniających wymagania :

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

Firewall.

Ochrony w warstwie aplikacji. Protokołów routingu dynamicznego. Redundancja, monitoring i wykrywanie awarii. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. W ramach postępowania system musi zostać dostarczony w postaci redundantnej. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN.

Interfejsy, Dyski:

System realizujący funkcję Firewall musi dysponować minimum 14 portami Gigabit Ethernet RJ-45, 2 gniazdami SFP 1 Gbps.

System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.

Parametry wydajnościowe:

W zakresie Firewall’a obsługa nie mniej niż 1,2 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 4 Gbps dla pakietów 512

B.Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 800 Mbps.Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA1: nie mniej niż 2,5 Gbps.

Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 1,5 Gbps.

Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps.

Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem AES256-SHA1) dla ruchu http – minimum 180 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

Kontrola Aplikacji.

Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.

Ochrona przed atakami - Intrusion Prevention System.

Kontrola stron WWW.

Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.

Zarządzanie pasmem (QoS, Traffic shaping).

Analiza ruchu szyfrowanego protokołem SSL.

Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

Polityki, Firewall

Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

System musi zapewniać 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.

W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

Wsparcie dla IKE v1 oraz v2.

Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM)

Obsługa protokołu Diffiego-Hellman grup 19 i 20

Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.

Tworzenie połączeń typu Site-to-site oraz Client-to-Site.

Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth

Mechanizm „Split tunneling” dla połączeń Client-to-Site

System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

Dla modułów: IPSec VPN oraz SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. Klient VPN musi umożliwiać weryfikację stanu bezpieczeństwa stacji zdalnej.

Rozwiązanie powinno zapewniać funkcjonalność VTEP (VXLAN Tunnel End Point)

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie powinno zapewniać obsługę:

 Routingu statycznego

 Policy Based Routingu

 Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Kontrola Antywirusowa

Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

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.

Ochrona przed atakami

Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

Kontrola aplikacji

Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P, Botnet.

Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontroli WWW

Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware, phishing, spam, Dynamic DNS, proxy avoidance.

Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.

Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie:

System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

Musi istnieć możliwość logowania do serwera syslog.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:

ICSA lub EAL4 dla funkcji Firewall

ICSA lub NSS Labs dla funkcji IPS

ICSA dla funkcji: SSL VPN, IPSec VPN

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

 Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres [60 ] miesięcy.

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania.

Zamawiający określił wymagania dotyczące routera CE w tabeli 6.1.2. W tabeli tej zostały wprowadzone zmiany i wymagania dotyczące routera zostały tam ostatecznie wyspecyfikowane.

5. Czy Zamawiający celem poprawienia konkurencyjności rozwiązania przy zachowaniu optymalnych kosztów, także przy możliwej rozbudowie rozwiązana w przyszłości ,dopuszcza zmiany w zapisach dotyczących „ Wymagania minimalne dotyczące macierzy dyskowej w zasobach lokalnych „

* + 1. Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active/active. Możliwość rozbudowy do 8 kontrolerów dyskowych tworzących jedną logiczną macierz bez konieczności wymiany zaoferowanej pary kontrolerów. Rozbudowa nie może odbywać się poprzez wirtualizację (podłączenie kilku macierzy przez wirtualizator zasobów dyskowych).

Czy Zamawiający dopuszcza rozwiązanie które posiada 2 kontrolery pracujące w trybie active/active które umożliwia zabezpieczanie konfiguracji dodatkową parą kontrolerów – klastra macierzy? Dwa kontrolery zapewniają odporność na awarię pojedynczego kontrolera. Ponadto klient nie określa wymaganej wydajności systemu dyskowego poprzez opis charakterystyki obciążeń wyrażonej w ilości operacji na sekundę (IOPS), wielkości bloku danych czy stosunku odczytów do zapisów na macierzy w związku z tym wymagana możliwość rozbudowy do 8 kontrolerów wydaje się nie być optymalna i przewymiarowana dla zastosowania związanego z budową środowiska.

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

* + 1. Rozbudowa oferowanej macierzy do co najmniej 500 napędów dyskowych, bez wymiany kontrolerów macierzowych (tylko poprzez dodanie półek i napędów dysków).

Czy zamawiający dopuści rozwiązanie które skaluje się w ramach pary kontrolerów do 264 dysków HDD/SSD a większa ilość dysków jest możliwa po wymianie kontrolerów? Zamawiający wymaga macierzy o pojemności 3.5TB zbudowanej z min. 9 dysków 1.2TB, wymagając jednocześnie możliwości rozbudowy do 500 dysków co oznaczało by, że zakłada potencjalny roczny przyrost danych na poziomie 120TB (wykorzystując dyski o tej samej pojemności i tego samego typu jak wymagane). W projekcie nie ma informacji uzasadniających zakładanych przyrostów danych ani wymaganej wydajności systemu dyskowego w związku z tym wymóg rozbudowy wydaje się być przewymiarowany.

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

* + 1. Min. 16 GB pamięci cache na każdy kontroler, pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości w pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min 48 godzin. Możliwość rozbudowy do 128 GB. Rozbudowa nie może odbywać się poprzez pamięć FLASH/SSD

Czy zamawiający dopuści macierz która oferuje możliwość rozbudowy do 32 GB cache na kontroler, bez konieczności rozbudowy do 128GB ? Wymóg określonej wielkości pamięci cache nie przekłada się bezpośrednio na wydajność macierzy, gdyż każdy producent może zaimplementować inne algorytmy wykorzystania pamięci cache i dostarczyć większą wydajność w IOPS z wykorzystaniem mniejszej pojemności pamięci cache

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

* + 1. Razem kontrolery muszą udostępnić minimum 8 interfejsów 1 Gb/s ETH i 8 interfejsów 10Gb/s FC/iSCSI do podłączenia sieci SAN. Możliwość rozbudowy o dodatkowe 8 interfejsy FC 8Gb/s lub 8 interfejsów 10Gb/s ETH.

Czy zamawiający dopuszcza rozwiązanie które posiada łącznie 8 portów iSCSI 10Gb? Rozwiązanie takie jest wystarczające w kontekście dostarczanego środowiska, i spójne z pozostałymi elementami rozwiązania.

Zamawiający zmienił zapisy SIWZ w tym zakresie.

* + 1. Wsparcie dla technologii klastrowania macierzy dyskowych (ang. Storage metro cluster) pozwalające na uruchomienie środowiska wysokiej dostępności (tryb activ-activ) zbudowanego z dwóch macierzy dyskowych. Dostarczenie wszystkich komponentów sprzętowych do uruchomienia w/w funkcjonalności dla środowisk wirtualizacyjnych. Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania.

Czy zamawiający dopuści rozwiązanie które wspiera technologię klastrowania macierzy dyskowych (ang. Storage Cluster) pozwalające na uruchomienie środowiska wysokiej dostępności zbudowanego z dwóch macierzy dyskowych? Oferowane rozwiązanie zapewni bezobsługową pracę aplikacji i systemów operacyjnych/wirtualizacyjnych oraz nie wymaga żadnej ingerencji w ich ustawienia.

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

* + 1. Minimum dwie karty Ethernet zapewniające min po dwa interfejsy (każda karta) 10Gb SFP+ wraz z min. 4 modułami optycznymi typu SR. Dodatkowa karta 1Gb Ethernet z min. 2 interfaceami.

Zamawiający wymaga aby serwery były podłączone bezpośrednio za pomocą kabli przyłączeniowych do macierzy – Wykonawca musi dostarczyć odpowiednie kable i interfacey sieciowe zarówno do serwerów jak i macierzy, jeśli zaproponowane rozwiązanie wymaga podłączenia za pośrednictwem dodatkowego przełącznika sieciowego, Wykonawca musi to uwzględnić w ofercie.

Czy w świetle powyższego zapisu, zakładając że serwery są wyposażone we wbudowane interfejsy 2x 1GbE, zamawiający wymaga zastosowania dodatkowej karty 2x 1GbE

Zamawiający zmienił zapisy SIWZ w tym zakresie.

6. 6.1.6.3 Wymagania minimalne dotyczące skanera małego

Zamawiający określił parametr: Rozdzielczość wyjściowa min. od 50 do 600 dpi. Dla prawidłowego podziału skanowanych pism na dokumenty systemy klasy EZD wykorzystują kody kreskowe. Skuteczne rozpoznawanie kodów oraz treści skanowanych obrazów przy 50 dpi jest niemożliwa do osiągnięcia.

Dlatego też wnosimy o zmianę tego parametru na:

Rozdzielczość wyjściowa: minimum 100 do 600 DPI

#### Zamawiający nie określił nigdzie w SIWZ, że będzie skanował kody kreskowe w rozdzielczości 50dpi. Podtrzymuje zapis SIWZ.

Zamawiający określił parametr Rozmiar dokumentów min. 50 mm x 50 mm. Zapis ten wskazuje tylko na jednego producenta skanerów dokumentowych jakim jest Avision. Zamawiający dokonał opisu parametrów technicznych w sposób utrudniający uczciwą konkurencję pomiędzy wykonawcami, co jest niedopuszczalne w świetle art. 29 ust. 2 Ustawy. Ten parametr spełnia tylko jeden producent – Avision.

W związku z tym wnosimy o zmianę tego parametru na:

Rozmiar dokumentów min. 52 mm x 52 mm, Maks. 216 mm x 356 mm.

#### Zamawiający zmienia minimalne rozmiary skanowanego dokumentu z 50mm x 50mm na nie wieksze niż 81mm x 81mm.

Zamawiający określił parametr: Prędkość skanowania min. 30 PPM / 60 IPM (dla: kolor, B&W, A4, 300 dpi), min. 40 PPM / 80 IPM (dla: kolor, B&W, A4, 200 dpi).

Wysoka jakość skanowanych kodów kreskowych oraz skuteczność rozpoznania OCR wymaga użycia trybu czarno białego i rozdzielczości 300 DPI. Powyższy zapis spełnia tylko jeden producent.

Wnosimy o zmianę tego parametru na: min. 40 PPM / 80 IPM (dla: kolor, B&W, A4, 300 dpi)

Prędkość skanowania przy rozdzielczości 200 dpi jest większa niż przy rozdzielczości 300 dpi, zatem jeżeli sprzęt Wykonawcy zapewnia większą prędkość skanowania przy rozdzielczości 200 dpi lub zapewnia tą prędkość przy większym niż 200 dpi, parametr zostanie spełniony. Zamawiający podtrzymuje zapis SIWZ.

Zamawiający określił parametr: Sugerowana obciążalność dzienna 5000 stron.

Prosimy o doprecyzowanie tego parametru, czy Zamawiający ma na myśli 5000 stron w co odpowiada 2 500 arkuszy dziennie w trybie duplex czy 5000 fizycznych arkuszy.

Parametr został wyraźnie określony jako „STRON”. Zatem wymagania spełnia skaner zapewniający obciążalność dzienną większą bądź równą skanowaniu 5000 arkuszy papieru jednostronnie [czyli 5000 stron] oraz taki który zapewnia 2500 arkuszy w trybie dwustronnym [czyli 5000 stron].

Zamawiający określił parametr: Interfejs min. USB 2.0

Obecnie stosowanym standardem komunikacyjnym dla skanerów dokumentowych jest USB 3.0, wszystkie nowoczesne komputery są wyposażone w taki port. USB 3.0 jako interfejs jest dużo szybszy od USB3.0 osiąga (600 MB/s) skutkiem czego gwarantuje szybszy transfer dokumentów ze skanera do stacji roboczej bez spowolnienia procesu skanowania spowodowanego niższą prędkością USB 2.0

 Prosimy o zmianę tego parametru na: Interfejs min. USB 3.0 kompatybilny z USB 2

Interface w standardzie USB 3.0 spełnia warunki minimalne zapisów SIWZ. Zamawiający podtrzymuje zapis SIWZ.

7. 6.1.6.4 Wymagania minimalne dotyczące skanera dużego

 Zamawiający określił parametr: Rozdzielczość wyjściowa min. od 50 do 600 dpi. Dla prawidłowego podziału skanowanych pism oraz dokumentów z systemy klasy EZD wykorzystują kody kreskowe. Skuteczne rozpoznanie kodów oraz treści skanowanych obrazów przy tak niskiej rozdzielczości jest niemożliwa do osiągnięcia.

 Dlatego prosimy o zmianę tego parametru na:

 Rozdzielczość wyjściowa: minimum 100 do 600 DPI.

#### Zamawiający nie określił nigdzie w SIWZ, że będzie skanował kody kreskowe w rozdzielczości 50dpi. Podtrzymuje zapis SIWZ.

 Zamawiający określił parametr: Rozmiar dokumentów min. 50 mm x 50 mm. Zapis ten wskazuje tylko na jednego producenta skanerów dokumentowych jakim jest Avision. Zamawiający dokonał opisu parametrów technicznych w sposób utrudniający uczciwą konkurencję pomiędzy wykonawcami, co jest niedopuszczalne w świetle art. 29 ust. 2 Ustawy. Ten parametr spełnia tylko jeden producent – Avision.

W związku z tym wnosimy o zmianę tego parametru na:

 Rozmiar dokumentów min. 52 mm x 52 mm, Maks. 216 mm x 356 mm

#### Zamawiający zmienia minimalne rozmiary skanowanego dokumentu z 50mm x 50mm na nie większe niż 81mm x 81mm.

 Zamawiający określił parametr: Prędkość skanowania min. 40 PPM / 80 IPM (dla: kolor, B&W, A4, 300 dpi), min. 60 PPM / 120 IPM (dla: kolor, B&W, A4, 200 dpi).

 Wysoka jakość skanowanych materiałów oraz odczyt kodów kreskowych oraz skuteczność rozpoznania OCR wymaga użycia trybu czarno białego i rozdzielczości 300 DPI. Powyższy zapis spełnia tylko jeden producent.

 Wnosimy o zmianę tego parametru na: min. 60 PPM / 120 IPM (dla: kolor, B&W, A4, 300 dpi)

Prędkość skanowania przy rozdzielczości 200 dpi jest większa niż przy rozdzielczości 300 dpi, zatem jeżeli sprzęt Wykonawcy zapewnia większą prędkość skanowania przy rozdzielczości 200 dpi lub zapewnia tą prędkość przy większym niż 200 dpi, parametr zostanie spełniony. Zamawiający podtrzymuje zapis SIWZ

 Zamawiający określił parametr: Sugerowana obciążalność dzienna 5000 stron.

 Prosimy o doprecyzowanie tego parametru, czy Zamawiający ma na myśli 5000 stron w co odpowiada 2 500 arkuszy dziennie w trybie duplex czy 5000 fizycznych arkuszy.

 Parametr został wyraźnie określony jako „STRON”. Zatem wymagania spełnia skaner zapewniający obciążalność dzienną większą bądź równą skanowaniu 5000 arkuszy papieru jednostronnie [czyli 5000 stron] oraz taki który zapewnia 2500 arkuszy w trybie dwustronnym [czyli 5000 stron].

Zamawiający określił parametr: Interfejs min. USB 2.0

Obecnie stosowanym standardem komunikacyjnym dla skanerów dokumentowych jest USB 3.0, wszystkie nowoczesne komputery są wyposażone w taki port. USB 3.0 jako interfejs jest dużo szybszy od USB3.0 osiąga (600 MB/s) skutkiem czego gwarantuje szybszy transfer dokumentów ze skanera do stacji roboczej bez spowolnienia procesu skanowania spowodowanego niższą prędkością USB 2.0

 Prosimy o zmianę tego parametru na: Interfejs min. USB 3.0 kompatybilny z USB 2

Interface w standardzie USB 3.0 spełnia warunki minimalne zapisów SIWZ. Zamawiający podtrzymuje zapis SIWZ.

8. Prosimy o określenie wymagań co do „dostawy serwera poczty wraz z oprogramowaniem”

Prosimy o określenie jakie jest przeznaczenie serwera poczty (jaką rolę ma pełnić w organizacji)?

Rolę serwera poczty e-mail.

Prosimy o określenie jaka funkcjonalność ma być dostępna dla użytkownika środowiska pocztowego np.: dostęp poprzez panel web, ?

Minimum: dostęp przez protokoły IMAPS, POP3S; dedykowany klient webmail; przechowywanie kalendarzy użytkowników, integracja użytkowników z LDAP/ActiveDirectory.

Prosimy o określenie czy w ramach serwera poczty ma być realizowana inna dodatkowa funkcjonalność, poza możliwością wysłania/odebrania poczty np.: praca grupowa, synchronizacja poprzez ActiveSync z urządzeniami mobilnymi?

Jak wyżej.

Prosimy o określenie jaki zakres funkcjonalności ma być dostępny dla panelu administracyjnego?

Minimum: zarządzanie kontami użytkownikow; zarządzanie aliasami; zarządzanie grupami użytkowników; zarządzanie ustawieniami usług pocztowych [np.: SMTP, POP3, IMAP, itd.]

Prosimy o określenie poprzez jakich klientów poczty mają się łączyć użytkownicy (web, aplikacja dostępowa, obie metody)?

Zarówno przez webmail i aplikację kliencką [np. Outlook, Thunderbird, itp.]

Prosimy o określenie co Zamawiający rozumie poprzez zapis: „Oprogramowanie serwera poczty e-mail”?

Przez zapis „Oprogramowanie serwera poczty e-mail” Zamawiający rozumie program lub zespół programów realizaujących zadania serwera poczty e-mail w zakresie opisanym powyżej.

Prosimy o określenie jak ma być realizowana usługa wsparcia dla serwera i jakiego okresu ona dotyczy?

Usługa wsparcia musi umożliwiać min.: pomoc lokalnym administratorom w instalacji i konfiguracji nowych instancji serwerów poczty; pomoc lokalnym administratorom w zarządzaniu incydentami z serwerem; pomoc lokalnym administratorom w bieżącej konserwacji systemu.

Prosimy o określenie jaki zakres dokumentacji ma zostać dostarczony po zrealizowaniu wdrożenia serwera poczty?

Dokumentacja w każdej części musi obejmować minimum instrukcję instalacji, konfiguracji, wykonywania kopii bezpieczeństwa i użytkowania. W zakresie użytkowania należy dostarczyć instrukcje zarówno dla użytkownika końcowego jak i administratora lokalnego. Dodatkowo należy dostarczyć opis wdrożeonej konfiguracji, tak aby możliwe było na jej podstawie odtworzenie środowiska po awarii.

Prosimy o określenie, czy występuje migracja poczty z lokalnych jednostek samorządowych na docelowy nowy serwer poczty? Jeżeli tak, to prosimy o podanie: nazwy systemu, z jakiego ma być zrealizowana migracja oraz ilości danych.

Ew. zadania migracji danych leżą po stronie Zamawiającego

Prosimy o określenie, czy ma wystąpić szkolenie administracyjne dla osób odpowiedzialnych za lokalną obsługę serwera? Jeżeli tak, to jaki ma być jego zakres?

Szkolenia obejmują swoim zakresem cały dostarczony System łącznie ze wszystkimi jego elementami, również serwera pocztowego w zakresie administrowania usługą.

Prosimy o informację, gdzie ma być umiejscowiona kopia zapasowa środowiska poczty realizowanego w wymienionych jednostkach samorządowych.

Na infrastrukturze w jednostkach samorządowych.

Prosimy o informację, czy w ramach funkcjonalności środowiska poczty ma być również realizowana funkcja archiwum pocztowego (lokalnie w jednostce samorządowej lub w zewnętrznym datacenter).

Jak wyżej.

Prosimy o informację, ilu użytkowników ma zostać utworzonych w ramach nowego środowiska poczty w każdej z wymienionych jednostek.

Zadanie tworzenia uzytkowników poczty spoczywa na Zamawiającym. Każdy serwer pocztowy musi umozliwiać obsługę min. 1000 kont pocztowych.

9. Wykonawca w punkcie „Świadczenie usługi serwisu” określił wymóg

„Wykonawca zapewni w godzinach pracy Zamawiającego w dni robocze obecność specjalistów mających niezbędną wiedzę i doświadczenie z zakresu eksploatacji Systemów”

Czy wyżej określony wymóg ma być realizowany przez fizyczną obecność specjalistów czy może być realizowany zdalnie ?

Zapis dotyczy usług świadczonych w ramach zdalnej pomocy.

10. Zamawiający w załączniku nr 2 do SIWZ wyspecyfikował :

7 Zakres 2. Dostawa Systemów EOD, Szyn Danych lokalnych i centralnej wraz z zestawem konektorów oraz Portalu Usług Elektronicznych

7.1 System EOD (EZD PUW)

EZD PUW – pozyskanie i wdrożenie systemu nie jest przedmiotem zamówienia. Zamieszczona dokumentacja interfejsu EZD służy jedynie zdefiniowaniu parametrów i zasad wymiany danych pomiędzy portalem E-usług i systemem EZD PUW.

oraz

7.4. Wdrożenie EOD, integracji i Lokalnych Szyn Danych

Wdrożenie ma na celu przeprowadzenie procesu umożliwiającego każdemu z partnerów korzystanie z lokalnej infrastruktury systemowej.

Oraz Zakres 2 Dostawa Systemów EOD (z wyłączeniem dostawy EZD PUW) oraz Szyny Danych wraz z zestawem konektorów u każdego z partnerów projektu na poziomie lokalnym. Dostawa portalu Usług elektronicznych oraz Szyny Danych na poziomie centralnym

Z uwagi na niejednoznaczne zapisy wnosimy Zamawiającego o informację czy wdrożenie System EOD jest przedmiotem zamówienia czy nie podlega dostawie i wdrożeniu.

Zamawiający w załączniku nr 2 do SIWZ wyspecyfikował:

 7.3. Usługi udostępnione dla poziomu centralnego

 W celu dostarczenia zaawansowanych usług elektronicznych dla mieszkańców i przedsiębiorców obszaru Wielkich Jezior Mazurskich konieczne jest dostarczenie usług integracji EOD i SD na potrzeby Portalu Usług Elektronicznych.

Prosimy o informację czy przedmiotem projektu jest fizyczna integracja SD na potrzeby Portalu Usług Elektronicznych czy tylko przygotowanie Portalu Usług Elektronicznych do integracji z SD. Jeżeli w ramach projektu Wykonawca musi przeprowadzić integrację rozwiązań prosimy o przekazanie dokumentacji API systemów wdrożonych u poszczególnych partnerów projektu.

Dla punktu 8 Zakres 3. Dostarczenie i wdrożenie formularzy elektronicznych

Wnosimy o przekazanie/wskazanie wzorów istniejących formularzy w formacie pdf lub doc np. na stronach BIP na potrzeby oszacowania kosztów wytworzenia formularzy elektronicznych. Ponadto prosimy o wskazanie w których formularzach mają być zastosowane walidacje pól oraz pola auto wyliczalne.

Jako, że system EZD PUW, ma być zainstalowany fizycznie na serwerach będących przedmiotem niniejszego zamówienia, niezbędna jest znajomość poniższych informacji przez potencjalnego Wykonawcę, celem doboru odpowiedniego rozwiązania sprzętowego. W związku z tym prosimy o określenie poniższych informacji technicznych:

Podesłanie minimalnym wymagań sprzętowych pod planowane wdrożenie EZD PUW

Określenie ile oraz jakie instancje systemu EZD PUW, zamawiający planuje wdrożyć. Czy Zamawiający planuje wdrożyć oprócz wersji szkoleniowej, również wersję testową?

Prosimy o podesłanie potencjalnej liczby pracowników ze wszystkich lokalizacji będących przedmiotem postępowania, którzy mają korzystać z licencji EZD PUW

Prosimy o podesłanie planowanego miesięcznego przyrostu danych z tytułu skanowanych dokumentów dla wszystkich lokalizacji .

Zamawiający wymaga uruchomienia EZD PUW na infrastrukturze dostarczonej przez Wykonawcę w ramach tego postępowania. Do zadań Wykonawcy należy również dostarczenie licencji na systemy operacyjne.

Wymagania minimalne do pracy EZD PUW:

dla serwera aplikacji:

- min 2 core 2 GHz

- min RAM 4 GB,

- min 50 GB przestrzeni dyskowej

dla serwera bazy danych:

- min. 2 core 2 GHz

- min 8GB RAM

- min. 50 GB przestrzeni dyskowej

- MS SQL Express 2016

Obydwa serwery wymagają systemu Windows Server.

11. Pytania i uwagi do CM-Zacznik\_nr\_2\_do\_SIWZ\_-\_SzOPZ.docx

Zamawiający w 6.1.1 Wymagania ogólne dot. dostarczanego sprzętu punkt WSZL19 opisuje funkcjonalności jakie mają zostać uruchomione, ale nie precyzuje zakresu ich konfiguracji. W szczególności nie opisuje konfiguracji Active Directory w zakresie : struktury, logiki, użytkowników, polityk GPO itp.

Dla tego prosimy o dopowiedz. Czy Zamawiający sam wykona szczegółową konfigurację tych rozwiązań na swoje potrzeby ? Czy Wykonawca ma takową konfigurację wykonać. Jeśli tak to na podstawie jakiego zakresu, ustaleń ?

Zamawiający wyznaczy administratorów lokalnych u każdego z Partnerów projektu w celu przeszkolenia ich przez Wykonawcę z w/w zakresu. Lokalni administratorzy po przeszkoleniu i z pomocą Wykonawcy stworzą wymaganą konfigurację.

Zamawiający w 6.11 Dostawa sprzętu nie precyzuje miejsca i sposobu wykonania montażu.

Czy Wykonawca może uznać, że po stronie Zamawiającego w dniu dostawy sprzętu będzie przygotowana przestrzeń w szafach rack, dostępne obwody zasilające itp. Do prawidłowego wykonania praca montażowych urządzeń ?

Zamawiający zagwarantuje wymaganą ilość w szafach RACK – do 42RU - i zapewni zasilanie po wcześniejszym powiadomieniu przez Wykonawcę zapotrzebowania w tym zakresie.

Zamawiający w 6.1.1 Wymagania ogólne dot. dostarczanego sprzętu punkt WSZL18 nie określa szczegółów dostawy sprzętu oraz ew. podłączenia do AD i migracji danych użytkowników.

Czy Wykonawca może założyć, że dostaw komputerów opisanych polega na dostawie i wypakowaniu urządzeń i podłączeniu ich ?

Zamawiający wymaga aby w zakresie dostawy i instalacji sprzętu odbyło się minimum:

1. Dostawa,
2. Wypakowanie,
3. Fizyczna instalacja w docelowym miejscu użytkowania,
4. Uruchomienie testowe sprzętu w celu sprawdzenia poprawności działania,
5. Utylizacja opakowań.

Podłaczenie do domeny wykona loklany administrator.

Zamawiający w 6.1.1 Wymagania ogólne dot. dostarczanego sprzętu punkt WSZL18 nie określa szczegółów dostawy sprzętu oraz ew. podłączenia do AD i migracji danych użytkowników. Czy Wykonawca może założyć, że dostaw komputerów opisanych polega na dostawie i wypakowaniu urządzeń i podłączeniu ich ?

Jak wyżej.

12. Zamawiający w punkcie 6.2Modernizacja sieci LAN nie określił następujących zagadnień

Dla tego prosimy o odpowiedź na pytania.

 Czy kabel użyty do zbudowania sieci musi być certyfikowany?

Kabel użyty do instalacji musi spełniać normy kategorii 5E.

 Czy obecne listy natynkowe muszą być odwzorowane (dotyczy producenta) czy wystarczy utrzymać wymiar?

Wystarczy utrzymać wymiar.

 Czy punkty PEL – gniazdka mogą być osadzone w kanałach listw natynkowych?

Tak

 Jaki kolor gniazdek ma być użyty do punktów elektrycznych „data” (białe/czerwone)?

Zamawiający zezwala na zastosowanie koloru czerwonego oraz niebieskiego.

 Czy rozbudowa o punkty elektryczne wymaga instalacji dodatkowych tablic bezpieczniku budujemy 12 punktów PEL)?

Według wiedzy Zamawiającego nie jest potrzebna instalacja dodatkowych rozdzielnic, ale wymagane jest instalowanie nowych zabezpieczeń w istniejących rozdzielnicach. Zamawiający zaleca do przeprowadzenia wizji lokalnej w tym zakresie w celu ustalenia faktycznych potrzeb. „Tabela 1. Ramowy wykaz dostarczanych rozwiązań do poszczególnych Partnerów Projektu” Zawiera pozycję „Sieć elektryczno-logiczna (liczba PEL do naprawy lub instalacji)” wskazującą na ilości nowo instalowanych bądź modernizowanych punktów sieci w poszczególnych jednostkach. Wszędzie tam, gdzie wskazno „0” nie wymaga się instalacji ani modernizacji punktów..

 Czy punkt PEL musi posiadać podwójne gniazdko LAN?

SIWZ określa: Zamawiający wymaga minimalnej struktury PEL : 1 gniazdo RJ45 + 1 gniazdo 230V.

 Jaka jest dostępność urzędów na wykonanie instalacji, tzn. kiedy można dokonywać odwiertów, montaży, tzw. „prac głośnych”?

W godzinach pracy Urzędu oraz po uzgodnieniu w dni robocze w godzinach wykraczających poza godziny pracy urzędów.

PAKIET 8

Pytanie 1

Dotyczy SIWZ, VIII. INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ LUB DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI, pkt. 6

*Zamawiający specyfikuje*:

Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert pod warunkiem, że wniosek o wyjaśnienie treści SIWZ wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.

Zamawiający wprowadził zmianę w związku z omyłką pisarską.

PYTANIE 1a: Zwracamy się z prośbą do Zamawiającego o wyjaśnienie powodów w zakresie ustanowienia 2 dni przed upływem terminu składania ofert na udzielenie wyjaśnień. Ustanowienie terminu udzielenia wyjaśnień na 2 dni przed upływem terminu składania ofert może wskazywać, że wartość zamówienia jest mniejsza niż kwoty określone w przepisach wydanych na podstawie art. 11 ust. 8 Pzp. Z kolei Zamawiający podaje w SIWZ, Rozdział II TRYB UDZIELENIA ZAMÓWIENIA w pkt. 2 ‘Wartość zamówienia przekracza kwotę określoną w przepisach wydanych na podstawie art. 11 ust. 8 ustawy Pzp.’, zatem zgodnie z art. 38 Ustawy PZP Zamawiający zobowiązany jest udzielić wyjaśnień nie później niż na 6 dni przed upływem terminu składania ofert.

Jak wyżej.

PYTANIE 1b: W związku z informację zawartą w SIWZ, Rozdział II TRYB UDZIELENIA ZAMÓWIENIA w pkt. 2 ‘Wartość zamówienia przekracza kwotę określoną w przepisach wydanych na podstawie art. 11 ust. 8 ustawy Pzp.’ Zwracamy się z prośbą do Zamawiającego o zmianę zapisów SIWZ w przywoływanym punkcie na: *Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 6 dni przed upływem terminu składania ofert pod warunkiem, że wniosek o wyjaśnienie treści SIWZ wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.*

Zamawiający wprowadził zmianę w związku z omyłką pisarską.

Pytanie 2

Dotyczy Umowa, § 3 PRZEDMIOT UMOWY, pkt. 10

Zamawiający specyfikuje:

Termin dostawy sprzętu, za wyjątkiem serwerów, macierzy i routerów, wynosi maksymalnie 30 dni od dnia zawarcia niniejszej umowy.

PYTANIE 2a: Co Zamawiający rozumie przez dostawę sprzętu, czy obejmuje ona usługę instalacji i konfiguracji?

Zamawiający wymaga aby w zakresie dostawy i instalacji sprzętu odbyło się minimum:

1. Dostawa,
2. Wypakowanie,
3. Fizyczna instalacja w docelowym miejscu użytkowania,
4. Uruchomienie testowe sprzętu w celu sprawdzenia poprawności działania,
5. Utylizacja opakowań.

PYTANIE 2b: Ze względu na dużą ilość zamawianych komputerów i laptopów dostawa przedmiotowego sprzętu w ciągu 30 dni jest wręcz niemożliwa. Szacunkowy czas od złożenia zamówienia do realizacji dla przedmiotowej liczby sprzętu u każdego z wiodących producentów wynosi około 4 tygodni. Mając na uwadze powyższe prosimy o wyłączenie z punktu §3.10 również stacji roboczych oraz stacji do centrum zarządzania.

Zamawiający wyraża zgodę na przesunięcie terminu zgodnie z powyższym.

Pytanie 3

Dotyczy Szczegółowego Opis Przedmiotu Zamówienia, punkt 10, Zakres 5. Przygotowanie i przeprowadzenie pakietów szkoleń, WSZ6, WSZ11 i WSZ12.

Zamawiający specyfikuje:

WSZ6 Zamawiający dopuszcza przeprowadzanie szkoleń grupowych, w grupach do 15 użytkowników oraz szkoleń indywidualnych przy stanowiskowych dla grup jedno-, dwu- lub trzyosobowych.

WSZ11 Zamawiający oczekuje przeprowadzenia szkoleń grupowych nie więcej niż:

- 10 dni szkoleń z zakresu integracji w warstwie Lokalnej Szyny Danych

WSZ12 Zamawiający oczekuje przeprowadzenia szkoleń grupowych w wymiarze:

- min. 5 dni szklenia z zakresu SUE, jednak nie większym niż 10 dni.

- min. 2 dni szkolenia dla Administratorów z zakresu SUE, jednak nie większym niż 5 dni.

PYTANIE 3a: Z przedstawionego przez Zamawiającego opisu wymagań w zakresie szkoleń, nie wynika jasno sprecyzowany czas jaki Wykonawca powinien poświęcić na przeprowadzenie szkoleń. Zamawiający specyfikuje, że dopuszcza przeprowadzenie szkoleń grupowych oraz indywidualnych, ale nie precyzuje ilość pracowników wymaganych do przeszkolenia zarówno w grupach do 15 użytkowników jak i szkoleń indywidualnych przy stanowiskowych dla grup jedno-, dwu- lub trzyosobowych.

Zwracamy się zatem z prośbą do Zamawiającego o podanie następujących informacji:

1. Szkolenia z zakresu integracji w warstwie Lokalnej Szyny Danych, w tym
	1. Ilość szkoleń grupowych, w grupach do 15 użytkowników
	2. Ilość szkoleń indywidualnych przy stanowiskach jednoosobowych
	3. Ilość szkoleń indywidualnych przy stanowiskach dwuosobowych
	4. Ilość szkoleń indywidualnych przy stanowiskach trzyosobowych

*Czy każde z powyższych szkoleń (a-d) powinno trwać 10 dni, czy łączna ilość dni dla wszystkich szkoleń wynosi 10 dni?*

Lokalna szyna danych nie jest przedmiotem zamówienia. Zamawiający skorygował zapisy SIWZ w tym zakresie (wymaganie WSZ11) EZD PUW nie wymaga instalacji dodatkowej szyny lokalnej ani centralnej.

1. Szkolenia z zakresu SUE, w tym
	1. Ilość szkoleń grupowych, w grupach do 15 użytkowników
	2. Ilość szkoleń indywidualnych przy stanowiskach jednoosobowych
	3. Ilość szkoleń indywidualnych przy stanowiskach dwuosobowych
	4. Ilość szkoleń indywidualnych przy stanowiskach trzyosobowych

*Czy każde z powyższych szkoleń (a-d) powinno trwać min. 5 dni, jednak nie więcej niż 10 dni, czy łączna ilość dni dla wszystkich szkoleń wynosi min. 5 dni, jednak nie więcej niż 10 dni?*

Nie dotyczy tego postepowania

1. Szkolenia dla Administratorów z zakresu SUE, w tym
	1. Ilość szkoleń grupowych, w grupach do 15 użytkowników
	2. Ilość szkoleń indywidualnych przy stanowiskach jednoosobowych
	3. Ilość szkoleń indywidualnych przy stanowiskach dwuosobowych
	4. Ilość szkoleń indywidualnych przy stanowiskach trzyosobowych

*Czy każde z powyższych szkoleń (a-d) powinno trwać min. 2 dni, jednak nie więcej niż 5 dni, czy łączna ilość dni dla wszystkich szkoleń wynosi min. 52dni, jednak nie więcej niż 5 dni?*

Szkolenia dotyczą wyłącznie Administratorów, obejmujące swoim zakresem wdrażane rozwiązania zgodnie z wymaganiami: WSZ7, WSZ8. Szkolenia certyfikowane nie są wymagane. Do przeszkolenia jest jedna grupa do 15 osób.

a)b)c)d) szkolenia opisane w WSZ7 i WSZ8. Zamawiający oczekuje propozycji liczby szkoleń, czasu ich trwania i szczegółowego programu, zgodnie z zapisem wymagania WSZ12.

Przykładowe tematy szkoleń :

|  |
| --- |
| Podstawy zarządzania bazami danych - MS SQL |
| Instalacja, konfiguracja i wdrożenie platformy Windows Serwer 2016 |
| Bezpieczeństwo w systemach sieciowych |

PYTANIE 3b: Czy Zamawiający wymaga przeprowadzenia innych szkoleń niż wymienionych w powyższym pytaniu? Jeżeli tak to zwracamy się z prośbą o wylistowanie tych szkleń z określeniem wymaganego minimalnego czasu na każde z wymaganych szkoleń.?

Zamawiający w ramach tego postępowania oczekuje przeprowadzenia jedynie szkoleń opisanych w SIWZ.

PYTANIE 4

Dotyczy SIWZ, V. Warunki udziału w postępowaniu pkt. II. e

Zamawiający specyfikuje:

„Specjalista ds. bezpieczeństwa informacji, posiadający wykształcenie wyższe oraz certyfikat zawodowy Audytora wiodącego Systemu Zarządzania Bezpieczeństwem Informacji oraz doświadczenie na stanowisku związanym z zapewnieniem bezpieczeństwa informacji systemów w sektorze publicznym, tj. posiada certyfikat Auditora ISE/IEC 27001:2013 w zakresie przetwarzanie danych osobowych w modelu cloud computing oraz uczestniczył w realizacji co najmniej dwóch usług polegających na przygotowaniu e-usług o wartości min. 2 000 000 zł brutto każdy.„

Pytanie 4a: Czy w nazwie certyfikatu wkradła się literówka w postaci zapisu: „certyfikat Auditora ISE/IEC 27001:2013”, podczas gdy Zamawiającemu chodziło o zapis: „certyfikat Auditora ISO/IEC 27001:2013”.

Oczywiście jest to omyłka pisarska, chodzi o certyfikat ISO

Pytanie 5

Dotyczy Szczegółowego Opis Przedmiotu Zamówienia,

Zamawiający specyfikuje: „System EOD (EZD PUW)

EZD PUW – pozyskanie i wdrożenie systemu nie jest przedmiotem zamówienia. Zamieszczona dokumentacja interfejsu EZD służy jedynie zdefiniowaniu parametrów i zasad wymiany danych pomiędzy portalem E-usług i systemem EZD PUW. Dokumentacja niezbędna do tego celu stanowi Załącznik nr 8 do SIWZ. „

Pytanie 5a: Prosimy o potwierdzenie, że dla żadnego z Partnerów nie jest konieczne dostarczenie EZD PUW ani innego systemu elektronicznego obiegu dokumentów.

Zamawiający potwierdza powyższy punkt.

Pytanie 5b: Prosimy o potwierdzenie, że dla żadnego z Partnerów nie jest konieczne uruchomienie EZD PUW ani innego systemu elektronicznego obiegu dokumentów.

Zamawiający potwierdza powyższy punkt.

Pytanie 5c: Prosimy o potwierdzenie, że w ramach zamówienia nie jest konieczna konfiguracja instancji EZD PUW, ani żadnego innego elektronicznego obiegu dokumentów.

Zamawiający potwierdza powyższy punkt.

Pytanie 5d: Jeśli Zamawiający wymaga dostarczenia elektronicznego obiegu dokumentów to prosimy o jego wyspecyfikowanie.

Zamawiający nie wymaga dostarczanie EZD PUW.

Pytanie 5e: Prosimy o informację, czy na dostarczonej infrastrukturze będzie docelowo uruchamiane EZD PUW lub inne rozwiązanie Elektronicznego Obiegu Dokumentów?

TAK, na dostarczanej infrastrukturze będzie uruchamiane EZD PUW.

Pytanie 6

Dotyczy Szczegółowego Opis Przedmiotu Zamówienia,

Zamawiający specyfikuje:

 „Warstwa Lokalnej Szyny Danych wraz z zestawem konektorów

Moduł przeznaczony jest do nadzoru nad integrowanymi danymi na poziomie lokalnym pomiędzy SD a EOD oraz umożliwiający udostępnienie danych z SD oraz EOD na potrzeby SUE centralnego.

(…)

Integracja ta ma na celu udostępnienie aktualnych informacji podatkowych (należności, płatności) oraz stan spraw urzędowych dla SUE. Integracja będzie możliwa do realizacji, o ile system EOD (PUW) będzie posiadał dostarczone interfejsy integracyjny w opisanym zakresie. W przypadku, kiedy PUW nie będzie posiadał poniższych możliwości integracyjnych, wówczas Wykonawca uzgodni dostarczenie integracji w momencie technicznej możliwości udostępnionej przez PUW w okresie gwarancji projektu. ”

Pytanie 6a: Prosimy o informację, jaka będzie ilość użytkowników Szyny danych?

Zamawiający wprowadził zmiany w SIWZ w tym zakresie. Nie wymaga dostarczenia Centralnej Szyny danych.

Pytanie 6b: Prosimy o potwierdzenie, ze wszystkie Systemy Dziedzinowe u Partnerów podsiadają niezbędne interfejsy umożliwiające realizację usług wyszczególnionych SIWZ.

Zamawiający potwierdza dostępność interfejsów do komunikacji w systemach SD Partnerow projektu. Integracja z SD nie jest przedmiotem tego postępowania

Pytanie 6c: Prosimy o potwierdzenie, że wykonawca nie będzie zobligowany do uiszczania jakichkolwiek opłat licencyjnych za użytkowanie usług dostępowych do SD Partnerów.

Moja propozycja odpowiedzi:

Integracja z SD nie jest przedmiotem tego postępowania

Pytanie 7

Wykonawca zwraca uwagę, że zapisy Szczegółowego Opis Przedmiotu Zamówienia są wewnętrznie niespójne. W jednym miejscu OPZ Zamawiający mówi o braku konieczności wdrożenia EZD, a poniższe zapisy:



Wskazują na uruchomienie EZD. Prosimy, zatem jednoznacznie wskazać:

Pytanie 7a: Czy wykonawca ma dostarczyć i uruchomić w ramach projektu jakikolwiek system EZD lub EOD?

W ramach tego postępowania nie jest wymagane dostarczenie systemu EOD. Powyższy zapis mówi jedynie o konieczności wykreowania odpowiednich maszyn wirtualnych w dostarczonycm środowisku.

Pytanie 7b:Jeśli odpowiedź na pytanie 7a jest twierdząca to:

* 1. ~~Jaka jest liczba użytkowników takiego systemu u każdego z Partnerów?~~
	2. ~~Jaka jest liczba dokumentów przychodzących i wychodzących, które będą przetwarzane u każdego z Partnerów?~~
	3. ~~Jaka jest ilość skanowanych dokumentów i wielkość plików zawierających skany dokumentów u każdego z Partnerów?~~
	4. ~~Jakie Zamawiający ma wymagania wobec systemu EZD lub EOD?~~
	5. ~~Co zdaniem Zamawiającego oznacza pojęcie – odpowiedni poziom bezpieczeństwa?~~

~~Wykonawca zwraca uwagę, że są to informacje podstawowe pozwalające na wymiarowanie rozwiązania, bez tych informacji niemożliwe jest oszacowanie pracochłonności w zakresie usług wdrożeniowych, ani wielkościowy dobór infrastruktury.~~

Pytanie 8

Dotyczy Szczegółowego Opis Przedmiotu Zamówienia,

Zamawiający specyfikuje:

|  |  |
| --- | --- |
| **WSDW16** | **Ze względu na zakładany dostęp do systemu z poziomu urządzeń mobilnych, strony systemu powinny automatycznie dostosowywać się do różnych rozdzielczości ekranu (Responsive Web Design).** |

Prosimy o potwierdzenie, że wymaganie to nie dotyczy rozwiązania szyny danych. Zdaniem wykonawcy stawianie tego wymagania wobec elementu ewidentnie back-office jest nadmiarowe i prowadzi do generowania zbędnych kosztów po stronie wykonawcy.

Zapis ten dotyczy Portalu Usług Elektronicznych.

Pytanie 9

Dotyczy Szczegółowego Opis Przedmiotu Zamówienia,

Zamawiający specyfikuje: :

„Zadaniem Wykonawcy jest dostarczenie formularzy dla Partnerów projektu, wg. Poniższego zapotrzebowania. O ile prawo centralne lub lokalnej nie wymaga inaczej, Wykonawca może zaproponować wspólne wzory i formularze dokumentów dla tych samych usług poszczególnym partnerom projektu.”

Prosimy o przekazanie tych wzorów formularzy, dla których wykonawca nie będzie mieć możliwości zaproponowania własnego układu. Dostarczenie wzorów na etapie przygotowania oferty jest niezbędne do prawidłowego oszacowania pracochłonności.

Zgodnie z wymaganiem WF2 to Wykonawca opracowuje formularz elektroniczny (zgodnie z właściwymi przepisami prawa) wykorzystując posiadane zasoby. Zamawiający po zakończeniu postępowania przedstawi wybranemu Wykonawcy tzw. „karty usług”, czyli opisy przebiegu realizowanych dotychczas procedur postępowania w jst. oraz ewentualnie stosowanych standardowych formularzy. Jednocześnie informujemy, że wszystkie wskazane e-formularze oraz opisy przebiegu procedur z nimi związanych są ogólnie dostępne na wielu portalach rządowych i samorządowych zatem Zamawiający zgodnie z wymaganiem WF14 dopuszcza możliwość wykorzystania przez Wykonawcę wzorów, które są już opublikowane w CRD. Jak wspomniano wyżej projekty e-formularzy będą wymagały wcześniejszego przedstawienia do zatwierdzenia Zamawiającemu.

Do celów szacowania wartości proszę skorzystać z centralnego repozytorium dokumentów.

Pytanie 10

Dotyczy Szczegółowego Opis Przedmiotu Zamówienia,

Zamawiający specyfikuje: Tabela 1. Ramowy wykaz dostarczanych rozwiązań do poszczególnych Partnerów Projektu

Pytanie 10a: Czy Partnera „Starostwo Powiatowe w Giżycku - 2 lokalizacje” należy traktować jako dwie lokalizacje i w związku z tym należy dostarczyć przykładowo po 2 szt. stanowisko robocze do każdej z lokalizacji, czyli razem 4sztuki dla Partnera?

Siedziba Powiatu Giżyckiego znajduje się w dwóch budynkach, logicznie stanowiących jeden Urząd i jedną sieć LAN.

Powiat Gizycki należy traktować jako jedną lokalizację z dwoma budynkami oddalonymi od siebie o około 500m.

Pytanie 11

Dotyczy Szczegółowego Opis Przedmiotu Zamówienia,

Zamawiający specyfikuje: 6.1.6.5 Wymagania dotyczące drukarki etykiet.

Pytanie 11a: Prosimy o określenie ilości drukarek etykiet, jakie należy dostarczyć w ramach postępowania?

12 szt, po jednej do każdej JST.

Pytanie 12.

Dotyczy – Załącznik nr 6 do Umowy

W pkt.7 Procedury podejmowania Prac Serwisowych Zamawiający wymaga odpowiednich czasów Realizacji Zgłoszenia Serwisowego.

Pytanie 12a) Prosimy o informację czy w przypadku Dysfunkcji związanej ze sprzętem czasy będą wynosiły zgodnie z WG17 OPZ „Terminy naprawy sprzętu są uzależnione od funkcji dostarczonego sprzętu i są podane w części specyfikacji sprzętu.”?

Jeśli Zamawiający nie wskazał w opisie sprzętu warunków serwisu należy przyjąć ogólne warunki ujęte w załączniku nr 6 do Umowy.

Pytanie 12b) Prosimy o wyjaśnienie nieścisłości związanej z wymaganym serwisem dla urządzeń (czas naprawy i czas reakcji) i zwracamy uwagę, że w przypadku większości sprzętów Zamawiający nie podał w specyfikacji czasów naprawy, w niektórych wskazał czasy reakcji.

Jeśli Zamawiający nie wskazał w opisie sprzętu warunków serwisu należy przyjąć ogólne warunki ujęte w załączniku nr 6 do Umowy.

Pytanie 13

Dotyczy Szczegółowego Opis Przedmiotu Zamówienia,

Zamawiający specyfikuje: 6.1.5 Wymagania minimalne dotyczące macierzy dyskowej w zasobach lokalnych. Dotyczy pkt.8 - Obsługiwane typy zabezpieczenia RAID

Zamawiający w pkt.8 wymaga aby zabezpieczenia RAID realizowane były za pomocą dedykowanego układu. W zdecydowanej większości dostępnych na rynku macierzy dyskowych obsługa RAID odbywa się z wykorzystaniem procesorów kontrolera, które zapewniają w tym celu niezbędną moc obliczeniową choćby poprzez większą ilość rdzeni procesora. Jednocześnie wydajności obu typów macierzy tzn. wykorzystujących dedykowane układy i tych wykorzystujących moc procesora nie odbiegają od siebie. Mając to na uwadze jak również fakt, że wymagana konfiguracja jest niewielka oraz nie posiada określonych jakichkolwiek wymagań wydajnościowych

*pytamy czy Zamawiający dopuści jako spełniające wymagania macierze realizujące zabezpieczenia RAID z użyciem procesorów kontrolera ?*

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

Pytanie 14

Dotyczy Szczegółowego Opis Przedmiotu Zamówienia,

Zamawiający specyfikuje: 6.1.5 Wymagania minimalne dotyczące macierzy dyskowej w zasobach lokalnych.

Zamawiający w wielu punktach zawarł wymagania odnośnie skalowalności rozwiązania – rozbudowa z 2 do 8 kontrolerów, rozbudowa do 500 dysków tylko poprzez dodanie półek i dysków, rozbudowa cache z 16 do 128 GB. Takie wymagania powodują, że koszt oferowanego rozwiązania będzie niewspółmiernie duży biorąc pod uwagę obecne wymagania czyli 2 kontrolery, cache 16 GB i 9 dysków. Bieżące wymaganie klasyfikują rozwiązanie jako rozwiązanie tzw. entry-level szczególnie, że Zamawiający nie podał żadnych wymagań wydajnościowych w odniesieniu do macierzy. Aby zachować skalowalność rozwiązania jednocześnie zapewniając ograniczenie zbędnych kosztów proponujemy w tej sytuacji ograniczenie wymagań dotyczących skalowalności.

*Pytanie 14a: Czy w związku z tym Zamawiający zgodzi się na następujące zapisy dotyczące skalowalności: rozbudowa do 4 kontrolerów, rozbudowa cache do 64 GB, rozbudowa do co najmniej 350 napędów dyskowych ?*

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

Pytanie 15

Dotyczy Szczegółowego Opis Przedmiotu Zamówienia,

Zamawiający specyfikuje: 6.1.8 Wymagania minimalne dotyczące oprogramowania do wirtualizacji serwerów lokalnych

Pytanie 15a: Prosimy o informację czy Zamawiający dopuści wersję oprogramowania do wirtualizacji posiadającego ograniczenie na ilość maksymalną ilość wirtualizowanych serwerów – np. paczka licencji na 3 serwery każdy 2 CPU oraz jedna konsola zarządzania?

Zamawiający wymaga możliwości uruchomienia dowolnej ilości maszyn wirtualnych.

Pytanie 16

Dotyczy Szczegółowego Opis Przedmiotu Zamówienia,

Zamawiający specyfikuje: 6.1.8 Wymagania minimalne dotyczące oprogramowania do wirtualizacji serwerów lokalnych – od pkt e Całkowite koszty posiadania - backup

Pytanie 16a: Prosimy o informację czy Zamawiający dopuści wersję oprogramowania do backupu posiadającego ograniczenie na ilość maksymalną ilość backupowanych serwerów oraz bez centralnej (jednej dla wszystkich partnerów projektu) konsoli zarządzającej – np. licencje na dostarczane serwery które mogą być rozbudowane do licencji na 3 serwery każdy 2 CPU?

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

Pytanie 16b: Jednocześnie prosimy o informację czy każdy z Partnerów posiada konto mailowe w innej domenie?

TAK, każdy partner posiada oddzielną domenę.

Pytanie 17

Dotyczy Szczegółowego Opis Przedmiotu Zamówienia,

Zamawiający specyfikuje: „Tabela 1. Ramowy wykaz dostarczanych rozwiązań do poszczególnych Partnerów Projektu”

Pytanie 17a) Prosimy o informację ile i w jakiej specyfikacji należy dostarczyć stacji zarządzających?

 Ilość wymagana została okrerślona w Tabeli 1 Załącznika nr 2 do SIWZ - SzOPZ.

Pytanie 17b) Czy mają to być urządzenia zgodne ze specyfikacją stacji roboczej?

Tak, stacje zarządzające mająbyć zgodne ze specyfikacją sprzętową stacji roboczej.

Pytanie 18

Dotyczy Specyfikacji Istotnych Warunków Zamówienia (SIWZ)

*Zamawiający specyfikuje:* Kryteria oceny ofert - odporność na awarie macierzy na poziomie

Zamawiający w przedmiotowym punkcie przyznaje dodatkowe punkty za „B – wyłączenie więcej niż jednego dysku nie powoduje utraty danych ani wydajności”. Pragniemy zwrócić uwagę, iż punkt ten zawiera błąd. W zaznaczonym zakresie znajdują się zarówno 2 dyski jak i wszystkie dyski w macierzy – prosimy o zmianę powyższego punktu na procentowy udział wyłączonych dysków

Zastosowany opis kryterium jest celowy, ma premiować rozwiązania bezpieczniejsze i pozostaje bez zmian.

Pytanie 19

Dotyczy Szczegółowego Opis Przedmiotu Zamówienia,

Pytanie 19a: Czy Zamawiający dopuszcza wizję lokalną w jednostkach, w których będą instalowane łącza, w celu dokonania oceny warunków technicznych dla instalacji wymaganych łączy?

Zgodnie z SIWZ, Zamawiający zaleca przeprowadzenie wizji lokalnych.

Pytanie 20

Dotyczy Szczegółowego Opis Przedmiotu Zamówienia,

Pytanie 20a: Czy dla lokalizacji znajdujących się pod wspólnym adresem, ale stanowiących odrębne jednostki administracyjne np. Giżycko, al. 1 Maja 14, konieczne będzie dostarczenie odrębnych (dwóch) łączy, czy wystarczy jedno o przepustowości 100 Mbps. ?

NIE. Z uwagi na odrębną osobowość i odrębny zakres działalności, pomimo wspólnego adresu należy te jednostki traktować jako dwie, zgodnie z SIWZ.

Pytanie 21

Dotyczy Szczegółowego Opis Przedmiotu Zamówienia, w pkt 9.6 Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy. Tabela 29 Parametry minimalne centralnej szyny danych oraz minimalny zakres usług bezpieczeństwa transferu danych.

Zamawiający specyfikuje: „ WD12: Wymagania zamawiającego dotyczące sieci WAN/MPLS przepustowość usług (…)”

Pytanie 21a: Czy stwierdzenie "wykonawca będzie świadczył usługę transmisji danych w oparciu o sieć IP/MPLS wykonawcy na bazie własnych łączy dostępowych routerów CE zainstalowanych w miejscach wskazanych przez zamawiającego" oraz Data Center wykonawcy, można rozumieć, jako infrastrukturę zapewnioną przez Wykonawcę?

Powyższy zapis SIWZ został zmieniony i w obecnym brzmieniu należy rozumieć ten zapis jako świadczenie usługi na łączach do których Wykonawca ma prawo użytkowania.

Pytanie 22

Dotyczy zapisów we wzorze umowy.

Zgodnie z par. 17 wzoru umowy „Wykonawca zobowiązuje się przenieść na Zamawiającego, autorskie prawa majątkowe albo udzielić licencji, do Oprogramowania Dedykowanego na następujących polach eksploatacji”.

Pytanie 22 a: Od czego zależy w/w zobowiązanie, które jest rozłączne („albo”),

tj. udzielenie licencji albo przeniesienie praw autorskich do Oprogramowania Dedykowanego?

W zależności od faktycznych możliwości Wykonawcy w tym zakresie, tj. od dysponowania prawami majątkowymi do wytworzonego orogramowania.

Pytanie 22 b: Co jest kryterium wyznaczającym zakres zobowiązania wykonawcy?

Jak wyżej.

Pytanie 23

Dotyczy zapisów w SIWZ. V. Warunki udziału w postępowaniu. I.WARUNKI UDZIAŁU W POSTĘPOWANIU.

*Zamawiający specyfikuje:*

*„Na podstawie art. 22c ust. 1 pkt. 1) i ust. 2 Zamawiający informuje, że wymóg ten jest pochodną szacunkowej wartości zamówienia, czasu jego realizacji. Zamawiający zakłada, z uwzględnieniem dwunastomiesięcznego okresu realizacji zamówienia, że ubiegać się o niniejsze zamówienie może tylko wykonawca, który wykaże łączny roczny obrót w obszarze objętym zamówieniem w wysokości 9.000.000 zł.”*

Pytanie 23a: Na jakiej podstawie, czy przyjmując jaki wskaźnik Zamawiający przyjął pochodną szacunkowej wartości zamówienia określając łączny obrót w obszarze objętym zamówieniem wysokość 9.000.000 zł?

Zgodnie z Art. 38. Ustawy Pzp, ust. 1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia.

Powyższy zapis nie jest pytaniem do treść SIWZ.

Pytanie 23b: W jaki sposób określono kwotę obrotu w wysokości 9.000.000zł, przyjmując tę kwotę jako pochodną szacunkowej wartości zamówienia?

Zgodnie z Art. 38. Ustawy Pzp, ust. 1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia.

Powyższy zapis nie jest pytaniem do treść SIWZ.

Pytanie 24

Dotyczy zapisów w SIWZ. V. Warunki udziału w postępowaniu.

*Zamawiający specyfikuje:*

*„Na każdym etapie postępowania, na podstawie art. 22d ust. 2 Ustawy Pzp, Zamawiający może uznać, że wykonawca nie posiada wymaganych zdolności, jeżeli uzna, że wskazane osoby są zaangażowane w inne przedsięwzięcia gospodarcze wykonawcy mogące mieć negatywny wpływ na realizację przedmiotowego zamówienia. Wykonawca będzie w tym wypadku zobowiązany do wskazania innych osób spełniających wymagania zamawiającego lub w przeciwnym wypadku zostanie wykluczony z postępowania.”*

Pytanie 24a: Na jakiej podstawie Zamawiający uzna, że wskazane osoby są zaangażowane w inne przedsięwzięcia gospodarcze u wykonawcy?

Zgodnie z art. 22d. ust 2 Ustawy PZP

Pytanie 24b: Na podstawie jakich kryteriów Zamawiający będzie oceniał negatywny wpływ, udziału osób w innych przedsięwzięciach gospodarczych Wykonawcy?

Zgodnie z art. 22d. ust 2 Ustawy PZP

Pytanie 25

Dotyczy zapisów w SIWZ rozdz. V ust. 2 dział II warunek e

*Zamawiający specyfikuje:*

*„Analityk posiadający wykształcenie wyższe oraz wiedzę i doświadczenie w planowaniu wdrażania systemów informatycznych, tj. posiada certyfikat OMG BPM lub TOGAF lub równoważny w odpowiednim zakresie oraz uczestniczył w realizacji co najmniej dwóch projektów polegających na przygotowaniu e-usług o wartości min. 2 000 000 zł brutto każdy.”*

Pytanie 25a: Jakiego poziomu certyfikatu OMG BPM lub TOGAF zamawiający wymaga  w powyższym warunku oraz co rozumie pod sformułowaniem: ”w odpowiednim zakresie”. ?

Zamawiający wymaga aby Analityk posiadał wiedzę i doświadczenie, więc w odniesieniu do certyfikatów musi posiadać poziom certyfikacji stwierdzający posiadaną wiedzę i doświadczenie w zekresie projektowania infrastruktury IT. Dla TOGAF będzie to „Poziom 2 - certyfikat potwierdza wiedzę oraz umiejętności praktyczne z zakresu TOGAF 9” dla OMG BPM – OCEB Technical Intermediate.

Pytanie 26

Dotyczy zapisów SIWZ rozdz. VII ust 5 pkt. 12) i 13)

*Zamawiający specyfikuje:„*

1. *dokumenty, o których mowa w ust. 1 pkt 1 i 6 powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.*
2. *dokumenty, o których mowa w ust 1 pkt 4 i 5 powinny być wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.„*

Pytanie 26a: Czy odniesienie do ust. 1 w punktach 12 i 13 stanowi omyłkę pisarską, a Zamawiający miał w tym punktach na myśli odniesienie do ust.5?

Zamawiający potwierdza, że powyższy zapis jest pomyłką i prawidłowe odniesienie powinno wskazywać na ust.5.

Pytanie 27

Dotyczy zapisów we wzorze umowy par 12 pkt. 5.2

*Zamawiający specyfikuje:*

 *„ 5.2.  świadczenie usług konsultacyjnych w dni robocze w godzinach 7.00 - 15.00 pod numerami telefonów określonymi § 11 ust. 5 Umowy;”*

Pytanie 27a: Czy Zamawiający w powyższym zapisie miał na myśli § 11 ust. 4 Umowy? Jeśli tak, prosimy o poprawienie treści wzoru umowy w tym zakresie.

Zamawiający wprowadził zmiany w Umowie.

Pytanie 28

Dotyczy zapisów we wzorze umowy par 12 pkt 14

*Zamawiający specyfikuje:*

 *„*

1. *Zamawiający może wypowiedzieć niniejszą Umowę w odniesieniu do Usług Utrzymania:*
	1. *z ważnych powodów – z zachowaniem 3-miesięcznego okresu wypowiedzenia. Za ważne powody uzasadniające wypowiedzenie Umowy przez Zamawiającego uznawane będą w szczególności następujące sytuacje:*
		1. *łączna suma kar umownych naliczonych przez Zamawiającego przekroczyła 10% wartości Umowy w części dotyczącej Usług Utrzymania;*
		2. *niedochowany został w danym miesiącu kalendarzowym Czas Naprawy Błędu Krytycznego więcej niż trzy razy;*
		3. *Wykonawca dopuścił się istotnego naruszenia postanowień Umowy, w szczególności w zakresie zasad przetwarzania danych osobowych, zasad zachowania poufności, dostarczenia Zamawiającemu rezultatów obarczonych wadami prawnymi;*
		4. *zaszły zmiany organizacyjne Zamawiającego skutkujące tym, że dalsze świadczenie Usług Utrzymania będzie nieuzasadnione gospodarczo.„*

Pytanie 28a : Par. 12 ust 14 odnosi się do podstaw wypowiedzenie przez Zamawiającego Umowy w zakresie Usług Utrzymania, w związku z czym wnioskujemy o modyfikację zapisów par 12 ust 14 ppkt 14.1.1 wzoru umowy tak, aby ppkt 14.1.1 odnosił się do zakresu Kar naliczanych za nienależyte wykonanie zobowiązań gwarancyjnych i usług utrzymania tj.: 14.1.1 łączna suma kar umownych naliczonych  Wykonawcy z tytułu par 21 ust. 11 umowy tj. nienależytego wykonania przez Wykonawcę zobowiązań gwarancyjnych i usług utrzymania , przekroczyła 10% wartości Umowy.

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

Pytanie 28b Par. 12 Wnioskujemy o usunięcie z treści wzoru umowy zapisów par 12 ppkt 14.1.2.

Mając na względzie wieloletnie doświadczenie w zakresie utrzymywania systemów informatycznych, sugerujemy, że Kategorie błędów w systemie zgłoszeniowym przyznawane są przez użytkowników często w oparciu o ich bieżące potrzeby, a nie w oparciu o definicje Błędów określone w umowie i wycenione przez Wykonawców na etapie przetargu. Wykonawcy w ramach dobrej współpracy rzadko kwestionują kategoryzacje błędów, lecz zapis par 12 ppkt 14.1.2 nakłada na Wykonawcę nie tylko ryzyko naliczenia wysokich kar, ale i wypowiedzenia umowy przez Zamawiającego, co może na etapie realizacji doprowadzić do niepotrzebnych konfliktów między stronami. Zamawiający zabezpieczył się już w par 12 ppkt 14.1.1 na wypadek niewywiązywania się Wykonawcy z obowiązków świadczenia w terminie usług serwisowych i nie widzimy podstaw do dublowania i tak już dużych restrykcji.

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

Pytanie 29

Dotyczy zapisów we wzorze umowy par 21 ust. 11 pkt 11.1

W związku z faktem, iż czas pracy opisany we wzorze umowy liczony jest odpowiednio w zdefiniowanych Dniach Roboczych i Godzinach Roboczych, wnosimy o modyfikację treści umowy zgodnie z poniższym:

11.1 w odniesieniu do Stanu Krytycznego – 200,00 PLN za każdą rozpoczętą Godzinę Roboczą opóźnienia.

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

Pytanie 30

Dotyczy Załącznika nr 6 do wzoru umowy Procedura podejmowania Prac Serwisowych Pkt 7 ppkt a

W związku z faktem, iż czas pracy opisany we wzorze umowy liczony jest odpowiednio w zdefiniowanych Dniach Roboczych i Godzinach Roboczych, wnosimy o modyfikację treści umowy zgodnie z poniższym:

* 1. 4 Godziny Robocze dla stanu krytycznego,

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

PAKIET 9

PYTANIE NR 1:

Zamawiający w pkt 9.6 WD13 wymaga aby:

Wykonawca zapewniał, że

1. posiada punkty styku z minimum dwoma operatorami działającymi na terenie Polski
2. posiada dostęp do minimum 150 systemów autonomicznych
3. posiada usługę Open peeling polegającą na wymianie ruchu i o parametrze co najmniej 150 uczestników i umożliwiającą podłączenie największych miastach Polski

Prosimy Zamawiającego o uzasadnienia takich wymagań na potrzeby projektu dla 12 podmiotów o liczbie mieszkańców nie przekraczającej 100 tys. Wydaje się bowiem, że tak wygórowane wymagania nie mają zastosowani w tym projekcie i są rażąco przeszacowane.

Zgodnie z Art. 38. Ustawy Pzp, ust. 1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia.

Powyższy zapis nie jest pytaniem do treść SIWZ.

PYTANIE NR 2:

Zamawiający w pkt 9.6 WD13 wymaga aby:

Wymagania minimalne dotyczące wydajności usługi Cloud Firewall:

* musi obsłużyć nie mniej niż 2 mln jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę.

Prosimy Zamawiającego o uzasadnienia takich wymagań na potrzeby projektu dla 12 podmiotów o liczbie mieszkańców nie przekraczającej 100 tys. Wydaje się bowiem, że tak wygórowane wymagania nie mają zastosowani w tym projekcie i są rażąco przeszacowane.

Zgodnie z Art. 38. Ustawy Pzp, ust. 1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia.

Powyższy zapis nie jest pytaniem do treść SIWZ.

PYTANIE NR 3:

Zamawiający w pkt 9.6 WD13 wymaga aby:

Wymagania minimalne dotyczące wydajności usługi Cloud Firewall:

* musi obsłużyć przepustowość Firewall na poziomie nie mniej niż 20 Gbps.

Prosimy Zamawiającego o uzasadnienia takich wymagań na potrzeby projektu dla 12 podmiotów o liczbie mieszkańców nie przekraczającej 100 tys. Wydaje się bowiem, że tak wygórowane wymagania nie mają zastosowani w tym projekcie i są rażąco przeszacowane.

Zgodnie z Art. 38. Ustawy Pzp, ust. 1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia.

Powyższy zapis nie jest pytaniem do treść SIWZ.

PYTANIE NR 4:

Zamawiający w pkt 9.6 WD13 wymaga aby:

Wymagania minimalne dotyczące wydajności usługi Cloud Firewall:

* musi obsłużyć przepustowość nie mniej niż 9 Gbps podczas połączeń szyfrowanych VPN IPSec.
* musi obsługiwać przepustowość minimum 6 Gbps podczas skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS)

Prosimy Zamawiającego o uzasadnienia takich wymagań na potrzeby projektu dla 12 podmiotów o liczbie mieszkańców nie przekraczającej 100 tys. Wydaje się bowiem, że tak wygórowane wymagania nie mają zastosowani w tym projekcie i są rażąco przeszacowane.

Zgodnie z Art. 38. Ustawy Pzp, ust. 1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia.

Powyższy zapis nie jest pytaniem do treść SIWZ.

PYTANIE NR 5:

Zamawiający w pkt 9.6 WD13 wymaga aby:

Wymagania minimalne dotyczące wydajności usługi Cloud Firewall:

* wydajność skanowania typowego ruchu z włączonymi funkcjami IPS, AC, AV musi obsługiwać minimum 1 Gbps.

Prosimy Zamawiającego o uzasadnienia takich wymagań na potrzeby projektu dla 12 podmiotów o liczbie mieszkańców nie przekraczającej 100 tys. Wydaje się bowiem, że tak wygórowane wymagania nie mają zastosowani w tym projekcie i są rażąco przeszacowane.

Zgodnie z Art. 38. Ustawy Pzp, ust. 1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia.

Powyższy zapis nie jest pytaniem do treść SIWZ.

PYTANIE NR 6:

Zamawiający w pkt 9.6 WD13 w pkt VI. System ochrony serwerów w JST wymaga, aby:

Usługa System ochrony serwerów w JST musi obsługiwać nie mniej niż 1 mln. jednoczesnych połączeń oraz 85 tys. nowych połączeń na sekundę.

Prosimy Zamawiającego o uzasadnienia takich wymagań na potrzeby projektu dla 12 podmiotów o liczbie mieszkańców nie przekraczającej 100 tys. Wydaje się bowiem, że tak wygórowane wymagania nie mają zastosowani w tym projekcie i są rażąco przeszacowane.

Zgodnie z Art. 38. Ustawy Pzp, ust. 1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia.

Powyższy zapis nie jest pytaniem do treść SIWZ.

PYTANIE NR 7:

Zamawiający w pkt 9.6 WD13 w pkt VI. System ochrony serwerów w JST wymaga, aby:

Usługa System ochrony serwerów w JST musi obsługiwać przepustowość Firewall na poziomie nie mniej niż 9 Gbps.

Prosimy Zamawiającego o uzasadnienia takich wymagań na potrzeby projektu dla 12 podmiotów o liczbie mieszkańców nie przekraczającej 100 tys. Wydaje się bowiem, że tak wygórowane wymagania nie mają zastosowani w tym projekcie i są rażąco przeszacowane.

Zgodnie z Art. 38. Ustawy Pzp, ust. 1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia.

Powyższy zapis nie jest pytaniem do treść SIWZ.

PYTANIE NR 8:

Zamawiający w pkt 9.6 WD13 w pkt VI. System ochrony serwerów w JST wymaga, aby:

Wydajność szyfrowania VPN IPSec musi obsługiwać nie mniej niż 850 Mbps.

Prosimy Zamawiającego o uzasadnienia takich wymagań na potrzeby projektu dla 12 podmiotów o liczbie mieszkańców nie przekraczającej 100 tys. Wydaje się bowiem, że tak wygórowane wymagania nie mają zastosowani w tym projekcie i są rażąco przeszacowane.

Zgodnie z Art. 38. Ustawy Pzp, ust. 1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia.

Powyższy zapis nie jest pytaniem do treść SIWZ.

PYTANIE NR 9:

Zamawiający w pkt 9.6 WD13 w pkt VI. System ochrony serwerów w JST wymaga, aby:

Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) musi obsługiwać minimum 3000 Mbps.

Prosimy Zamawiającego o uzasadnienia takich wymagań na potrzeby projektu dla 12 podmiotów o liczbie mieszkańców nie przekraczającej 100 tys. Wydaje się bowiem, że tak wygórowane wymagania nie mają zastosowani w tym projekcie i są rażąco przeszacowane.

Zgodnie z Art. 38. Ustawy Pzp, ust. 1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia.

Powyższy zapis nie jest pytaniem do treść SIWZ.

PYTANIE NR 10:

Zamawiający w pkt 9.6 WD13 w pkt VI. System ochrony serwerów w JST wymaga, aby:

Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami IPS, AC, AV musi obsługiwać minimum 1500 Mbps.

Prosimy Zamawiającego o uzasadnienia takich wymagań na potrzeby projektu dla 12 podmiotów o liczbie mieszkańców nie przekraczającej 100 tys. Wydaje się bowiem, że tak wygórowane wymagania nie mają zastosowani w tym projekcie i są rażąco przeszacowane.

Zgodnie z Art. 38. Ustawy Pzp, ust. 1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia.

Powyższy zapis nie jest pytaniem do treść SIWZ.

PYTANIE NR 11:

Zamawiający w pkt 9.6 WD13 w pkt VI. System ochrony serwerów w JST wymaga, aby:

Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDoS.

Prosimy Zamawiającego o uzasadnienia takich wymagań na potrzeby projektu dla 12 podmiotów o liczbie mieszkańców nie przekraczającej 100 tys. Wydaje się bowiem, że tak wygórowane wymagania nie mają zastosowani w tym projekcie i są rażąco przeszacowane.

Zgodnie z Art. 38. Ustawy Pzp, ust. 1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia.

Powyższy zapis nie jest pytaniem do treść SIWZ.

PYTANIE NR 12:

Zamawiający w pkt 9.6 WD13 w pkt VI. System ochrony serwerów w JST wymaga, aby:

System logowania i raportowania udostępniony w usłudze Cloud Firewall musi być przystosowany do współpracy z usługą Ochrony serwerów w JST. Udostępniony System logowania i raportowania musi umożliwiać kolekcjonowanie logów z co najmniej 200 urządzeń.

Prosimy Zamawiającego o uzasadnienia takich wymagań na potrzeby projektu dla 12 podmiotów o liczbie mieszkańców nie przekraczającej 100 tys. Wydaje się bowiem, że tak wygórowane wymagania nie mają zastosowani w tym projekcie i są rażąco przeszacowane.

Zgodnie z Art. 38. Ustawy Pzp, ust. 1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia.

Powyższy zapis nie jest pytaniem do treść SIWZ.

PYTANIE NR 13:

Zamawiający w pkt 10 wymaga, aby:

„Szkolenia mają na celu osiągniecie odpowiedniej wiedzy z zakresu używania systemu na odpowiednich stanowiskach służbowych. Przeprowadzenie pakietu szkoleń powinno zostać odpowiednio skoordynowane z przeprowadzeniem procesu wdrożenia, a w szczególności z procedurą migracji danych”

O jakiej migracji mowa ?

Zamawiający ma na myśli wszystkie migracje danych, jakie będą konieczne do wykonania na etapie wdrożenia w celu uruchomienia i prawidłowego działania dostarczonego Systemu, np. danych serwerów pocztowych.

PAKIET 10

PYTANIE NR 1:

Zamawiający w Załączniku nr 2 do SIWZ — Szczegółowy Opis Przedmiotu Zamówienia w pkt. 6.3.3- Wymagania minimalne punktów dostępowych wskazuje:

*„1. Punkt dostępozvy musi być dedykowanym urządzeniem sieciowym przystosowanym do montowania na zewnątrz budynku [klasa min. IP67].(...)*

*(...)*

*2. Wymagane parametry fizyczne: (...)*

1. *Slot karty SIM* z *modułem pracującym w standardzie LTE/4G (...)*
2. *Temperatura pracy min. od -40 do +60 °C*

(*...)*

*10. Zamawiający wymaga aby do każdego punktu WiFi dostarczone zostały karty SIM zezwalające na nielimitowany dostęp do internetu za pomocą technologii LTE w okresie trwałości projektu."*

W ofercie żadnego producenta nie występuje tego typu dedykowane urządzenie wykonane w obudowie typu IP67 i posiadające slot na karty SIM z modułem LTE/4G. Ponadto w ofercie żadnego producenta nie występuje tego typu urządzenie w standardowej obudowie przeznaczone do pracy w warunkach "indor, a dysponujące wymaganym modułem i slotem SIM.

Jedyną możliwością implementacji wymaganych funkcjonalności są urządzenia bezprzewodowe dysponujące portem USB obsługującym modem USB LTE/4G wyposażony w slot karty SIM. Jednak tego typu urządzenie w żadnym wypadku nie spełnia wymagań do pracy zewnętrznej (zarówno samo urządzenie bezprzewodowe, jak i modem LTE oraz samo połączenie tych urządzeń poprzez USB), w docelowych warunkach wyznaczonych przez Zamawiającego.

W związku z powyższymi, czy Zamawiający dopuści rozwiązanie, które będzie składało się z poniższych elementów:

1. bezprzewodowego punktu dostępowego przeznaczonego do użytku wewnętrznego -typu indoor o temperaturze pracy O do +50 °C, dysponującego wbudowanymi antenami, wbudowanym portem USB oraz umożliwiającego pracę w trybie autonomicznym jak również w trybie cienkiego punktu dostępowego zarządzanego przez dedykowany kontroler,
2. zewnętrzny modern 4G USB, znajdujący się na oficjalnej liście kompatybilności urządzeń producenta stosowanego punktu dostępowego, oraz dostępnego w oficjalnym kanale sprzedaży na terenie Unii Europejskiej, oraz dostępnego w oficjalnym kanale sprzedaży polskich operatorów sieci 4G/LTE
3. obudowy mieszczącej bezprzewodowy punkt dostępowy wraz z modemem 4G zamocowanym bezpośrednio lub za pośrednictwem odpowiedniego przedłużacza USB,która będzie przystosowana do montażu rozwiązania na zewnątrz budynku (ścianie lub uchwycie), a która będzie posiadała klasę odporności IPX 5 oraz zakres temperatury pracy -20 do +50 °C, a tym samym będzie w stanie zapewnić bezpieczeństwo pracy obu urządzeń w realnie występujących warunkach atmosferycznych?

Według wiedzy Zamawiającego na rynku występują tego typu urządzenia. Zamawiający dopuści jednak rozwiązanie polegające na montażu punktu dostępowego bądź routera z funkcją Access Pointa z dołączonym modemem 4G/LTE w szczelnej obudowie i przystosowanych do pracy w warunkach atmosferycznych występujących na tej szerokości geograficznej, pod warunkiem zachowania innych zapisów SIWZ w tym zakresie oraz dostarczenia modemów 4G/LTE przystosowanych do pracy ciągłej.

PAKIET 11

Pytanie 1

W załączniku nr 2 do SIWI, punkt 9.6 Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy, cześć WD13 Bezpieczeństwo i ochrona przed atakami, Zamawiający wskazał wymagania w zakresie usługi Ochrony przed atakami. Uprzejmie zwracamy uwagę, że w specyfikacji brak jest wymagań technicznych identyfikujących oczekiwaną wydajność ochrony przed atakami aplikacyjnymi i wolumetrycznymi typu DoS.

Czy Zamawiający w zakresie ochrony przed atakami wolumetrycznymi typu DoS, zaakceptuje rozwiązanie umożliwiające zabezpieczenie punktu styku z siecią publiczną przed atakami o wolumenie do 20 Gbps i 20 Mpps?

Czy Zamawiający w zakresie ochrony przed atakami aplikacyjnymi typu DoS, zaakceptuje rozwiązanie umożliwiające zabezpieczenie punktu styku z siecią publiczną przed atakami do 1 Gbps i 1 Mpps?

Zamawiajacy dopuści zaproponowane rozwiązanie.

Pytanie 2

W załączniku nr 2 do SIWZ, punkt 9.6 Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy, cześć WD13 Bezpieczeństwo i ochrona przed atakami, Zamawiający wskazał wymagania w zakresie usługi Systemu ochrony serwerów w JST. Prosimy o potwierdzenie, że Zamawiający wymaga zainstalowania na każdym z lokalnych fizycznych serwerów w JST, systemu ochrony serwerów (o wymaganiach wyspecyfikowanych przez Zamawiającego) pod postacią maszyny wirtualnej (VM) realizującej funkcję ochrony maszyn wirtualnych posadowionych na danym fizycznym serwerze JST.

Zamawiajacy dopuści zaproponowane rozwiązanie.

Pytanie 3

W załączniku nr 2 do SIWZ, punkt 9.6 Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy, cześć WD13 Bezpieczeństwo i ochrona przed atakami, Zamawiający wskazał wymagania w zakresie usługi Cloud Firewall. Biorąc pod uwagę dużą złożoność projektu obejmującego kilkanaście JST oraz znaczną ilość użytkowników wewnętrznych jak i zewnętrznych, wymóg w zakresie ilości 130 tyś. nowych połączeń na sekundę wydaje się wielkością niedoszacowaną. Przy tak złożonym projekcie, wydaje się, że parametr ten powinien oscylować na poziomie co najmniej 250 tyś. nowych połączeń na sekundę. W przeciwnym wypadku użytkownicy wewnętrzni będą mieli znacząco ograniczony dostęp do wewnętrznych zasobów JST, a użytkownicy zewnętrzni mogą utracić możliwość połączenia z portalem E-usług.

W związku z powyższym, czy Zamawiający podniesie wielkość parametru ze 130 do 250 tyś. nowych połączeń na sekundę?

Zamawiający pozostawi zapis bez zmian, zaoferowanie urządzeń oferujących lepsze parametry niż minimalne wymagane nie spowoduje odrzucenia oferty.

Pytanie 4

W załączniku nr 2 do SIWZ, punkt 9.6 Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy, cześć WD13 Bezpieczeństwo i ochrona przed atakami, Zamawiający wskazał wymagania w zakresie usługi Cloud Firewall. Prosimy o potwierdzenie, że wymaganie w zakresie obsługi przepustowość Firewall na poziomie nie mniej niż 20 Gbps dotyczy zarówno pakietów UDP o małych rozmiarach (64byte) jak i rozmiarach średnich (512 byte) jak i dużych (1518 byte), a nie dotyczy tylko dużych pakietów UDP.

Tak , dotyczy wszystkich typów pakietów

Pytanie 5

W załączniku nr 2 do SIWZ, punkt 9.6 Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy, cześć WD13 Bezpieczeństwo i ochrona przed atakami, Zamawiający wskazał wymagania w zakresie usługi Cloud Firewall. W szczególności Zamawiający wymaga dostarczenia usługi Cloud Firewall w oparciu o system bezpieczeństwa znajdujący się na terenie Polski, co jest w pełni zrozumiałe w świetle założeń projektu. Jednocześnie w ramach usługi Wykonawca musi udostępnić centralny system logowania i raportowania. W celu zapewnienia spójności architektury rozwiązania oraz zagwarantowania odpowiedniego poziomu bezpieczeństwa systemu zasadne jest zagwarantowanie składowania oraz archiwizacji logów również na terenie Polski.

Prosimy o potwierdzenie, że wymóg lokalizacji na terenie Polski dotyczy również centralnego systemu logowania i raportowania.

Zamawiający dopuszcza zastosowanie systemu logowania na terenie UE, czyli również Polski.

Pytanie 6

W załączniku nr 2 do SIWZ, punkt 9.6 Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy, cześć WD13 Bezpieczeństwo i ochrona przed atakami, Zamawiający wskazał wymagania w zakresie usługi Web Application Firewall (WAF). Zwracamy uwagę, w specyfikacji brak jest wymagań technicznych parametryzujących wydajność usługi klasy WAF. Czy Zamawiający zaakceptuje rozwiązanie umożliwiające realizacje usługi Web Application Firewall spełniającej poniższe wymogi:

* Obsługa ruchu nieszyfrowanego w warstwie 4 do 6 Gbps;
* Obsługa ruchu nieszyfrowanego w warstwie 7 do 6 Gbps;
* Obsługa ruchu szyfrowanego przy długości klucza 2048 do 6 Gbps;
* Minimalna ilość połączeń na sekundę w warstwie 4 do 630 000 CPS;
* Minimalna ilość zapytań na sekundę w warstwie 7 do 850 000 RPS;
* Minimalna ilość połączeń SSL na sekundę przy długości klucza 2048 do 2 300 CPS;
* Minimalna ilość połączeń SSL na sekundę przy kluczu EC-P256 do 9 000 CPS?

Zamawiający zaakceptuje powyższe rozwiązanie.

Pytanie 7

W załączniku nr 2 do SIWZ, punkt 9.6 Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy, cześć WD13 Bezpieczeństwo i ochrona przed atakami, Zamawiający wskazał wymagania w zakresie usługi Secure Cloud Mail Gateway (SCMG). Czy Zamawiający dopuści rozwiązanie Secure Cloud Mail Gateway umożliwiające obsługę lokalnych skrzynek pocztowych użytkowników, które pracować będzie w trybie gateway (relay) dla serwera SMTP, a nie w trybie lokalnego serwera poczty?

Zamawiający zaakceptuje powyższe rozwiązanie.

Pytanie 8

W załączniku nr 2 do SIWZ, punkt 9.6 Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy, cześć WD13 Bezpieczeństwo i ochrona przed atakami, Zamawiający wskazał wymagania w zakresie usługi Secure Cloud Mail Gateway (SCMG), która musi zapewnić obsługę nieograniczonej ilość skrzynek pocztowych Zamawiającego. Zwracamy uwagę, że systemy bezpieczeństwa służące do realizowania ochrony skrzynek pocztowych posiadają zdefiniowane ilości skrzynek pocztowych, które mają chronić. Czy Zamawiający dopuści rozwiązanie, które chroni zdefiniowaną ilość lokalnych skrzynek pocztowych Zamawiającego? W przypadku akceptacji propozycji rozwiązania, czy Zamawiający uzna za spełniające wymagania rozwiązanie zdolne obsłużyć do 1000 lokalnych skrzynek pocztowych w ramach architektury SCMG?

Zamawiający dopuści rozwiązanie obsługujące minimum 1000 skrzynek pocztowych .

Pytanie 9

W załączniku nr 2 do SIWZ, punkt 9.6 Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy, cześć WD13 Bezpieczeństwo i ochrona przed atakami, Zamawiający wskazał wymagania w zakresie usługi Secure Cloud Mail Gateway (SCMG), która musi zapewnić obsługę wszystkich domen pocztowych Zamawiającego — bez limitu ilości. Zwracamy uwagę, że systemy bezpieczeństwa służące do realizowania ochrony domen pocztowych posiadają zdefiniowane ilości domen, które mają chronić. Czy Zamawiający uzna za spełniające wymagania rozwiązanie zdolne obsłużyć do 100 domen pocztowych Zamawiającego w ramach architektury SOMO?

Zamawiajacy dopuści rozwiązanie obsługujące minimum 100 domen Zamawiającego.

Pytanie 10

W załączniku nr 2 do SIWZ, punkt 9.6 Integracja z szyną danych oraz zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy, cześć WD13 Bezpieczeństwo i ochrona przed atakami, Zamawiający wskazał wymagania w zakresie usługi Secure Cloud Mail Gateway (SOMO) polegających na możliwość zdefiniowania co najmniej 200 profili antywirusowych oraz możliwość zdefiniowania co najmniej 200 profili antyspamowych. Prosimy o potwierdzenie, że ilość 200 profili antywirusowych oraz 200 profili antyspamowych, jest liczona w ramach całej architektury SCMG.

Zamawiajacy potwierdza, że liczba profili odnosi się do całej architektury SCMG w rozumieniu chmurowej ochrony poczty e-mail.

PAKIET 12

Pytanie 1

Załącznik nr 2 do SIWZ, Punkt 2.2; Zamawiający wprowadza w dokumentacji termin „System dziedzinowy (SD) definiowany jako:

„Oferowany przez Wykonawcę zintegrowany system informatyczny dedykowany do obsługi działalności JST” Prosimy o wyjaśnienie czy dostawa i wdrożenie Systemów dziedzinowych (SD) dla beneficjentów projektu jest przedmiotem zamówienia?

Zwracamy uwagę, że dostawa Systemów dziedzinowych nie została uwzględniona w tabeli 1 „Ramowy wykaz dostarczanych rozwiązań…”

W przypadku odpowiedzi twierdzącej, proszę o wyjaśnienie jakie są wymagania

unkcjonalne/pozafunkcjonalne Zamawiającego w odniesieniu do tego systemu i jak w szczególności należy interpretować oczekiwany zakres SD jako systemu dedykowanego do obsługi działalności JST

Przedmiotem tego postępowania nie jest dostawa systemuów SD ani EZD PUW.

Pytanie 2

Załącznik nr 2 di SIWZ, Punkt 2.1; Zgodnie z opisem przedmiotu zamówienia określonym przez

Zamawiającego:

„Na poziomie lokalnym, tj. u każdego z Partnerów projektu zostanie dostarczony i wdrożony system Elektronicznego Obiegu Dokumentów wraz z Szyną Danych lub zestawem konektorów. Wykonawca dostarczy integrację rozwiązania Elektronicznego Obiegu Dokumentów z System Dziedzinowym Partnera poprzez Szynę Danych lokalną/dedykowane konektory programowe”

Prosimy o wyjaśnienie, czy Zamawiający ma w tym miejscu na myśli integrację z Systemem Dziedzinowym Partnera dostarczonym przez Wykonawcę w ramach realizacji przedmiotowego zamówienia czy istniejącym/będącym w eksploatacji Systemem Dziedzinowym Partnera?

W przypadku wymogu integracji z obecnie eksploatowanymi Systemami Dziedzinowymi Partnerów prosimy

o:

a) wskazanie dla jakich Systemów Dziedzinowych Partnerów Wykonawca powinien dostarczyć integrację – proszę o wskazanie nazw produktów i producentów

b) potwierdzenie, że Zamawiający i Partnerzy projektu zapewnią dostosowanie eksploatowanych przez siebie Systemów Dziedzinowych do komunikacji/współpracy z usługami Lokalnej Szyny Danych dostarczonej przez Wykonawcę

Przedmiotem tego postępowania nie jest dostawa systemuów SD ani EZD PUW.

Pytanie 3

SIWZ pkt. III, Załącznik 2 do SIWZ pkt. 2 i pkt; Zgodnie z opisem przedmiotu zamówienia wskazanym w pkt 2 Załącznika 2 do SIWZ Na str. 4

„Na poziomie lokalnym, tj. u każdego z Partnerów projektu zostanie dostarczony i wdrożony system Elektronicznego Obiegu Dokumentów wraz z Szyną Danych lub zestawem konektorów”

W tabeli na str. 12

Zakres 2 -

Jednocześnie, w podpunkcie 7.1 punktu 7 OPZ zatytułowanego jako „ Dostawa Systemów EOD, Szyn Danych lokalnych i centralnej wraz z zestawem konektorów oraz Portalu Usług Elektronicznych” Zamawiający poprzez określenie „System EOD (EZD PUW)” dokonuje zrównania definicji System EOD i EZD PUW oraz stanowi ,że „EZD PUW - pozyskanie i wdrożenie systemu nie jest przedmiotem zamówienia…” W aspekcie powyższych niejednoznacznych zapisów OPZ, prosimy o jednoznaczne wyjaśnienie:

1) Czy przedmiot zamówienia obejmuje dostawę i wdrożenie systemów EOD?

2) Czy przedmiot zamówienia obejmuje jakiekolwiek działania Wykonawcy dot. wdrożenia systemu EZD PUW?

3) Jakie inne systemy EOD „ z wyłączeniem dostawy EZD PUW) są przedmiotem Zakresu 2 realizacji zamówienia?

Przedmiotem tego postępowania nie jest dostawa systemuów SD ani EZD PUW.

Zamawiający zmienił zapisy SIWZ w tym zakresie.

PAKIET 13

Pytanie 1.

Czy Zamawiający jest zobligowany przestrzegać artykułu 29 uPZP:

1. Przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględniając wszystkie wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty.

2. Przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję?

Zgodnie z Art. 38. Ustawy Pzp, ust. 1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia.

Powyższy zapis nie jest pytaniem do treść SIWZ.

Pytanie 2.

Wszystkie wymagania Zamawiającego jednoznacznie wskazują na macierz Huawei OceanStor 5300 V3, której specyfikację można znaleźć na stronie producenta pod adresem:

http://e.huawei.com/en/products/cloud-computing-dc/storage/unified-storage/mid-range

Czy Zamawiający ma zamiar kupić macierz Huawei OceanStor 5300 V3?

W opisie przedmiotu zamówienia Zamawiający opisał swoje wymagania dotyczące dostarczanych urządzeń i rozwiązań. Ustawa Pzp nie nakłada na Zamawiającym konieczności znajomości wszystkich rozwiązań dostępnych na rynku. Niemniej jednak Zamawiajacy wie, że są przynajmniej dwa konkurencyjne rozwiązania innych firm spełniające w/w wymagania.

Pytanie 3.

Załącznik nr 2 do SIWZ Tabela 4 Wymagania minimalne dotyczące macierzy dyskowej w zasobach lokalnych, Pkt 2

Zamawiający wymaga, aby model zaoferowanej macierzy był wyposażony w 2 kontrolery a równocześnie miał „możliwość rozbudowy do 8 kontrolerów dyskowych tworzących jedną logiczną macierz bez konieczności wymiany zaoferowanej pary kontrolerów. Rozbudowa nie może odbywać się poprzez wirtualizację (podłączenie kilku macierzy przez wirtualizator zasobów dyskowych).”

Zamawiający tym wymaganiem znacząco ogranicza konkurencję dopuszczając wyłącznie macierz dyskową firmy Huawei OceanStor 5300 V3.

Wymaganie rozbudowy do 8 kontrolerów zupełni nie przystaje do pierwotnie zamawianej konfiguracji dyskowej (Zamawiający chce zakupić macierz mającą tylko 9 dysków). Najprostsze 2-kontrolerowe macierze klasy midrange entry-level wszystkich producentów obsługują ponad 100 dysków, co ponad 10-krotnie przekracza obecne wymagania Zamawiającego. Macierze klasy midrange średniej klasy potrafią obsłużyć ponad 500 dysków (w tym przypadku macierz OceanStor wyposażona w 8 kontrolerów obsłuży 2000 dysków). Formułowanie takich wymagań, znacznie przekraczających realne potrzeby Zamawiającego to jawny przykład naruszenia uczciwej konkurencji i wskazanie na konkretne rozwiązanie.

Czy Zamawiający, chcąc zapewnić uczciwą konkurencję, zaakceptuje model macierzy wyposażony w 2 kontrolery, który umożliwi późniejszą rozbudowę (bez konieczności zakupu dodatkowych licencji i konieczności migracji danych) do 1000 dysków?

Zaproponowane rozwiązanie – macierz wyposażona w 2 kontrolery obsługujące do 1000 dysków – jest rozwiązaniem spełniającym minimalny wymóg określony w SIWZ – czyli obsługę min. 500 dysków.

Pytanie 4

Załącznik nr 2 do SIWZ Tabela 4 Wymagania minimalne dotyczące macierzy dyskowej w zasobach lokalnych, Pkt 4

Zamawiający wymaga, aby model zaoferowanej macierzy obsługiwał minimum 500 dysków. Taka ilość jest niewspółmiernie duża do zamawianej pierwotnie konfiguracji dyskowej (Zamawiający chce zakupić macierz mającą 9 dysków) i zakłada jej rozbudowę o ponad 5500%, co praktycznie nie zdarza się w świecie IT. W taki sposób Zamawiający naraża się na zarzut niegospodarności przy wydatkowaniu środków publicznych.

Czy Zamawiający, chcąc zapewnić uczciwą konkurencję, zaakceptuje model macierzy obsługujący 150 dysków, umożliwiający jednocześnie rozbudowę polegającą jedynie na wymianie kontrolerów (bez konieczności zakupu dodatkowych licencji i konieczności migracji danych) do modelu obsługującego do 1000 dysków?

Zaproponowane rozwiązanie – macierz wyposażona w 2 kontrolery obsługujące do 1000 dysków – jest rozwiązaniem spełniającym minimalny wymóg określony w SIWZ – czyli obsługę min. 500 dysków. Jednakże Zamawiajacy wymaga zachowania możliwości rozbudowy macierzy bez potrzeby wymiany dostarczonej pary kontrolerów.

Pytanie 5.

Załącznik nr 2 do SIWZ Tabela 4 Wymagania minimalne dotyczące macierzy dyskowej w zasobach lokalnych, Pkt 8

Zamawiający wymaga poziomu zabezpieczenia danych RAID 0, jednak RAID 0 nie wprowadza żadnego zabezpieczenia danych, bo w przypadku awarii jakiegokolwiek dysku nastąpi CAŁKOWITA UTRATA DANYCH niezależnie od ilości posiadanych dysków hot spare.

Wnosimy, aby dla zapewnienia uczciwej konkurencji Zamawiający usunął wymagania na wsparcie dla RAID 0?

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.

Pytanie 6.

Załącznik nr 2 do SIWZ Tabela 4 Wymagania minimalne dotyczące macierzy dyskowej w zasobach lokalnych, Pkt 14

Zamawiający wymaga wsparcia dla technologii tworzenia klastra storage, nie wymagając tej funkcjonalności. Jednocześnie wymaga dostarczenia wszystkich komponentów sprzętowych do uruchomienia tej funkcjonalności. Takie wymaganie w nieuczciwy sposób promuje rozwiązanie firmy Huawei OceanStor 5300 V3. Różni producenci oferują różne typy rozwiązań klastrowych budowanych w oparciu o różne komponenty sprzętowe i programowe. Takie sformułowanie wymagań spowoduje, że Zamawiający zakupi sprzęt, którego być może nigdy nie wykorzysta, czym naraża się na zarzut niegospodarności przy wydatkowaniu środków publicznych.

Dla zapewnienia uczciwej konkurencji wnosimy usunięcie z wymagania następującego zdania:

„Dostarczenie wszystkich komponentów sprzętowych do uruchomienia w/w funkcjonalności dla środowisk wirtualizacyjnych”.

Zamawiający podtrzymuje zapisy SIWZ w tym zakresie.