



**Fundusze  
Europejskie**  
Polska Cyfrowa



**Rzeczpospolita  
Polska**

**Unia Europejska**  
Europejski Fundusz  
Rozwoju Regionalnego



RI.271.5.2022.AM

**Zamawiający:**

Gmina Lipowa  
ul. Wiejska 44  
34-324 Lipowa

### **Odpowiedzi na pytania**

dotyczy: postępowania RI.271.5.2022.AM o udzielenie zamówienia publicznego  
prowadzonego w trybie podstawowym bez przeprowadzenia negocjacji pn.

**Dostawa sprzętu informatycznego realizowana w ramach projektu „Cyfrowa Gmina”.**

Na podstawie art.284.ust.3, w związku z art.284.ust.1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2021 r. poz. 1129 ze zm.), Zamawiający udziela wyjaśnień na złożone zapytania do Specyfikacji Warunków Zamówienia(SWZ) w przedmiotowym postępowaniu:

#### **Pytanie nr 1**

W opisie przedmiotu zamówienia widnieje zapis:

„Kliknięcie na wskazaną przez narzędzie aplikację musi powodować wyświetlenie wszystkich komputerów, na których dany program został wykryty.”

„Musi wyszukiwać nieaktualne wersje oprogramowania na stacjach roboczych i serwerach.”

Czy zamawiający dopuszcza rozwiązanie posiadające moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. Moduł skanujący działa bezpośrednio na urządzeniu, bez konieczności instalowania agenta na komputerach w sieci. Moduł nie tylko wykrywa oprogramowanie ale również wykrywa i informuje o lukach i podatnościach występujących w wykrytym oprogramowaniu.

#### **Odpowiedź:**

**Zamawiający dopuszcza rozwiązanie posiadające moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie.**

#### **Pytanie nr 2**

„W ramach filtra www muszą być dostępne m.in. kategorie: spyware, malware, spam, proxy avoidance, sieci społecznościowe, zakupy.”



Czy zamawiający dopuszcza rozwiązanie, w którym nie ma kategorii spyware i proxy avoidance, ale jest 8 innych kategorii poświęconych bezpieczeństwu jak: Anonymizers (Strony działające jako automatyczne przekierowania do innych stron), Compromised (Strony zagrażające bezpieczeństwu urządzenia, np. wymuszające instalację złośliwego oprogramowania bez wiedzy użytkownika), Phishing & Fraud (Strony używane do zwodniczych lub nielegalnych celów (np. phishing), takich jak pomoc przy wykradaniu finansowych lub osobistych informacji), Spam Sites, Malware, Translators (Strony tłumaczące witryny internetowe lub frazy z jednego języka na inny. Strony pozwalające na ominięcie zapory proxy, łączące się z wystąpieniem ryzyka nieautoryzowanego dostępu.), Botnets, Hacking,

**Odpowiedź:**

Zamawiający dopuszcza rozwiązanie, w którym nie ma kategorii spyware i proxy avoidance, ale jest 8 innych kategorii poświęconych bezpieczeństwu jak:

Anonymizers (Strony działające jako automatyczne przekierowania do innych stron), Compromised (Strony zagrażające bezpieczeństwu urządzenia, np. wymuszające instalację złośliwego oprogramowania bez wiedzy użytkownika), Phishing & Fraud (Strony używane do zwodniczych lub nielegalnych celów (np. phishing), takich jak pomoc przy wykradaniu finansowych lub osobistych informacji), Spam Sites, Malware, Translators (Strony tłumaczące witryny internetowe lub frazy z jednego języka na inny. Strony pozwalające na ominięcie zapory proxy, łączące się z wystąpieniem ryzyka nieautoryzowanego dostępu.), Botnets, Hacking.

**Pytanie nr 3**

Pytanie do: załącznik nr 2 OPZ > CZĘŚĆ 1 – DOSTAWA INFRASTRUKTURY SERWEROWEJ> V Zasilacz awaryjny UPS

Opis Zamawiającego:

" Zakres częstotliwości napięcia wejściowego: 50/60 Hz  $\pm$  3%."

Czy Zamawiający dopuści urządzenie z zakresem częstotliwości 45 ÷ 55 Hz  $\pm$  1 Hz?

**Odpowiedź:**

Zamawiający dopuszcza urządzenie z zakresem częstotliwości napięcia wejściowego 45 ÷ 55 Hz  $\pm$  1 Hz.

**Pytanie nr 4**

Pytanie do: załącznik nr 2 OPZ > CZĘŚĆ 1 – DOSTAWA INFRASTRUKTURY SERWEROWEJ> V Zasilacz awaryjny UPS

Opis Zamawiającego:

" Zniekształcenie napięcia wyjściowego < 5%"

Czy Zamawiający dopuści urządzenie ze zniekształceniem napięcia wyjściowego < 10%?



**Odpowiedź:**

**Zamawiający nie dopuszcza urządzeń ze zniekształceniem napięcia wyjściowego < 10%. Zamawiający podtrzymuje zapisy SWZ.**

**Pytanie nr 5**

Pytanie do: załącznik nr 2 OPZ > CZĘŚĆ 1 – DOSTAWA INFRASTRUKTURY SERWEROWEJ> V  
Zasilacz awaryjny UPS

*Opis Zamawiającego:*

*" Zakres napięcia wyjściowego 220V/230V/240V"*

Czy Zamawiający dopuści urządzenie obejmujące zakres napięcia tylko do 230V?

**Odpowiedź:**

**Zamawiający dopuszcza urządzenie obejmujące zakres napięcia wyjściowego do 230V**

**Pytanie nr 6**

Pytanie do: załącznik nr 2 OPZ > CZĘŚĆ 1 – DOSTAWA INFRASTRUKTURY SERWEROWEJ> V  
Zasilacz awaryjny UPS

*Opis Zamawiającego:*

*" Sprawność minimum 93%"*

Czy Zamawiający dopuści urządzenie o sprawności 90%?

**Odpowiedź:**

**Zamawiający nie dopuszcza urządzeń o sprawności 90%. Zamawiający podtrzymuje zapisy SWZ.**

**Pytanie nr 7**

Pytanie do: załącznik nr 2 OPZ > CZĘŚĆ 1 – VI. System ochrony danych UTM

*Opis Zamawiającego:*

- *Kliknięcie na wskazaną przez narzędzie aplikację musi powodować wyświetlenie wszystkich komputerów, na których dany program został wykryty.*

- *Musi wyszukiwać nieaktualne wersje oprogramowania na stacjach roboczych i serwerach*

Czy Zamawiający dopuszcza rozwiązanie posiadające moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. Moduł skanujący działa bezpośrednio na urządzeniu, bez konieczności instalowania agenta na komputerach w sieci.

Moduł nie tylko wykrywa oprogramowanie ale również wykrywa i informuje o lukach i podatnościach występujących w wykrytym oprogramowaniu

**Odpowiedź:**



**Zamawiający dopuszcza rozwiązanie posiadające moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie.**

Pytanie nr 8

Pytanie do: załącznik nr 2 OPZ > CZĘŚĆ 1 – VI. System ochrony danych UTM

*Opis Zamawiającego:*

- *W ramach filtra www muszą być dostępne m.in. kategorie: spyware, malware, spam, proxy avoidance, sieci społecznościowe, zakupy*

Czy Zamawiający dopuszcza rozwiązanie, w którym nie ma kategorii spyware i proxy avoidance, ale jest 8 innych kategorii poświęconych bezpieczeństwu jak:

Anonymizers (Strony działające jako automatyczne przekierowania do innych stron), Compromised (Strony zagrażające bezpieczeństwu urządzenia, np. wymuszające instalację złośliwego oprogramowania bez wiedzy użytkownika), Phishing & Fraud (Strony używane do zwodniczych lub nielegalnych celów (np. phishing), takich jak pomoc przy wykradaniu finansowych lub osobistych informacji), Spam Sites, Malware, Translators (Strony tłumaczące witryny internetowe lub frazy z jednego języka na inny. Strony pozwalające na ominięcie zapory proxy, łączące się z wystąpieniem ryzyka nieautoryzowanego dostępu.), Botnets, Hacking.

Odpowiedź:

Zamawiający dopuszcza rozwiązanie, w którym nie ma kategorii spyware i proxy avoidance, ale jest 8 innych kategorii poświęconych bezpieczeństwu jak:

Anonymizers (Strony działające jako automatyczne przekierowania do innych stron), Compromised (Strony zagrażające bezpieczeństwu urządzenia, np. wymuszające instalację złośliwego oprogramowania bez wiedzy użytkownika), Phishing & Fraud (Strony używane do zwodniczych lub nielegalnych celów (np. phishing), takich jak pomoc przy wykradaniu finansowych lub osobistych informacji), Spam Sites, Malware, Translators (Strony tłumaczące witryny internetowe lub frazy z jednego języka na inny. Strony pozwalające na ominięcie zapory proxy, łączące się z wystąpieniem ryzyka nieautoryzowanego dostępu.), Botnets, Hacking.

Pytanie nr 9

Pytanie do: załącznik nr 2 OPZ > CZĘŚĆ 1 – VI. System ochrony danych UTM

Większość opisanych przez Zamawiającego funkcji bezpieczeństwa w urządzeniach klasy UTM jest możliwa do realizacji poprzez posiadanie odpowiedniej licencji. Licencje udzielane są na dany okres czasu. Prosimy o informacje na jaki okres czasu Zamawiający wymaga aby licencja została uruchomiona.?

Odpowiedź:

**Zgodnie z SWZ, załącznik 4, §8 pkt3.**



Pytanie nr 10

W opisie funkcjonalności rozwiązania dla części 1. Zamawiający wymaga, aby serwer posiadał:

„Zintegrowana karta graficzna o rozdzielczości minimum 1920x1200”

Czy w celu zwiększenia konkurencyjności Zamawiający dopuści rozwiązanie wyposażone w zintegrowaną kartę graficzną o rozdzielczości 1280x1024?

Odpowiedź:

**Zamawiający dopuści rozwiązanie wyposażone w zintegrowaną kartę graficzną o rozdzielczości 1280x1024.**

Pytanie nr 11

W opisie funkcjonalności rozwiązania dla części 1. Zamawiający wymaga, aby serwer posiadał:

„Minimum 4 sloty PCIe generacji 3.0, w tym minimum 2 sloty o prędkości x16”

Czy w celu zwiększenia konkurencyjności Zamawiający dopuści rozwiązanie wyposażone w minimum 4 sloty PCIe generacji 3.0, w tym 1 slot o prędkości x16”?

Odpowiedź:

**Zamawiający dopuści takie rozwiązanie wyposażone w minimum 4 sloty PCIe generacji 3.0, w tym 1 slot o prędkości x16”**

Pytanie nr 12

W opisie funkcjonalności rozwiązania dla części 1 Zamawiający określił funkcjonalności dla systemu kopii zapasowych.

Prosimy o doprecyzowanie, czy Zamawiający dopuści rozwiązanie licencjonowane czasowo oraz dostarczone w postępowaniu na okres min. 5 lat z możliwością dalszego, płatnego przedłużenia?

Odpowiedź:

**Minimalny okres gwarancji został określony w SWZ. W okresie gwarancji wykonawca musi zapewnić wsparcie serwisowe oraz dostęp do aktualizacji systemu. Gwarancja musi być zgodna z warunkami określonymi w SWZ.**

Pytanie nr 13

W opisie funkcjonalności rozwiązania dla części 1. Zamawiający wymaga, aby system kopii zapasowych posiadał:

„Jeden procesory wielordzeniowy, osiągające w teście PassMark CPU Mark wynik min. 17.000 punktów według wyników ze strony [http://www.cpubenchmark.net/cpu\\_list.php](http://www.cpubenchmark.net/cpu_list.php)”



Czy w celu zwiększenia konkurencyjności Zamawiający dopuści rozwiązanie, które w teście PassMark CPU Mark osiąga wynik 10.000 punktów?

**Odpowiedź:**

**Zamawiający nie dopuszcza rozwiązania, którego procesor w teście PassMark CPU Mark osiąga wynik 10.000 punktów.**

**Pytanie nr 14**

W opisie funkcjonalności rozwiązania dla części 1. Zamawiający wymaga, aby system kopii zapasowych posiadał: „Możliwość instalacji dysków twardych minimum SATA, SAS, SSD.”

Czy w celu zwiększenia konkurencyjności Zamawiający dopuści rozwiązanie bez możliwości instalacji dysków twardych typu SAS?

**Odpowiedź:**

**Zamawiający nie dopuszcza systemu kopii zapasowych bez możliwości instalacji dysków twardych typu SAS.**

**Zamawiający podtrzymuje zapisy SWZ.**

**Pytanie nr 15**

W opisie funkcjonalności rozwiązania dla części 1. Zamawiający wymaga, aby stacja robocza posiadała:

„minimum 8 portów USB wyprowadzonych na zewnątrz komputera w tym min 4 porty USB w wersji 3.2; min. 2 porty USB w wersji 3.2 z przodu obudowy.”

Czy w celu zwiększenia konkurencyjności Zamawiający dopuści rozwiązanie które będzie posiadało 7 portów USB wyprowadzonych na zewnątrz komputera, zachowując przy tym zapis min. 4 porty USB w wersji 3.2; min. 2 porty USB w wersji 3.2 z przodu obudowy?

Pragniemy zauważyć iż do pracy biurowej nie jest potrzebna tak duża ilość portów USB, a w/w zapis skutecznie ogranicza zasady konkurencyjności zapisane w ustawie Pzp.

**Odpowiedź:**

**Zamawiający dopuści takie rozwiązanie.**

Zatwierdził: Wójt Gminy Jan Góra

  
Jan Góra