**Załącznik Nr 1 do SIWZ**

Dostawa serwera typ 1 – ilość: 1 szt.

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Producent : ………………………………………..

Nazwa lub model: ..………………………………………

**Rok produkcji: 2018**

|  |  |  |
| --- | --- | --- |
| Lp. | **OPIS** | **PARAMETRY OFEROWANE - opisać, wypełnić\*** |
| 1. **PARAMETRY WYMAGANE** | | |
|  | **Obudowa**  Obudowa w rozmiarze 1U przystosowana do montażu w szafie rack19”, wyposażona w teleskopowe szyny montażowe i prowadnice kabli, umożliwiającą instalację min. 4 HDD z ramka zabezpieczającą LCD | \* |
|  | **Płyta główna**  Przystosowana do pracy z procesorami serwerowymi. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. | \* |
| 3. | **Chipset**  Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych | \* |
| 4. | **Procesor**  procesor wyposażony w10 rdzeni z taktowaniem zegara min. 2.40Ghz osiągający w teście wydajności PassMarkAverage CPU Mark co najmniej 15 300 punktów, pracującyw architekturze 64 bit przystosowany do pracy w środowisku o wysokim współczynniku obciążenia i zapotrzebowania na zasoby obliczeniowe. Procesor musi obsługiwać wszystkie, aktualnie dostępne technologie wirtualizacyjne, opracowane przez producenta danego procesora.  Wynik testu dostępny pod adresem <https://www.cpubenchmark.net>  Zamawiający zastrzega sobie prawo do dokonanie weryfikacji parametrów oferowanego procesora na dzień otwarcia ofert poprzez wydrukowanie ze strony <https://www.cpubenchmark.net> testu wydajności.  W przypadku uzyskania w teście wydajności na dzień otwarcia ofert wartości niższych niż oferowane **oferta będzie podlegała odrzuceniu.** | \*Podać wydajność procesora:  …………………………………. |
| 5. | **RAM**  Nie mniej niż **64GB**, Wymagane jest zaoferowanie najszybszej (dla oferowanego modelu serwera) wersji pamięci operacyjnej dostępnej w ofercie producenta oferowanego serwera i w pełni kompatybilnej z zaoferowanym procesorem. | \*Podać pojemność:  ……………………………………….. |
| 6. | **Interfejsy sieciowe**  4 porty RJ-45 GbE | \* |
| 7. | **Napęd optyczny**  Wewnętrzny napęd DVD+/-RW | \* |
| **8.** | **Dyski twarde**  Możliwość instalacji dysków SATA, SAS oraz SSD 3,5‘‘. Zainstalowane, co najmniej 4 dyski twarde   * 2 x 200GB SSD * 2 x 300GB SAS 15k | \* |
| 9. | **RAID**   * Typ kontrolera Sprzętowy * Poziomy RAID 0,1,5,10,50 * obsługa dysków SATA, SAS, SSD * Transfer 12Gb/s | \* |
| 10. | **Porty**   * 4 x USB * VGA, * 1port szeregowy (RS – 232-C) | \* |
| 11. | **Video**  Zintegrowana karta graficzna. wyście D-SUB | \* |
| 12. | **Zasilacze**  Dwa niezależne źródła zasilania; redundantne – zdolne do obsługi awarii jednego źródła zasilania przy ciągłym dostarczeniu mocy niezbędnej do zasilenia serwera. W każdym przypadku procesory serwerów winny pracować z nominalną, maksymalną częstotliwością. Możliwość wymiany zasilaczy bez potrzeby odłączania kabla doprowadzającego zasilanie do obudowy. | \* |
| 13. | **Bezpieczeństwo**  Zintegrowany z płytą główną moduł TPM | \* |
|  | **Zarządzanie**  Dedykowany moduł zdalnego zarzadzania, diagnostyki i monitorowania pracy serwera. **Zarządzanie realizowane poprzez dedykowany port** | Podać czas pracy:  ……………………………………….. |
|  | **Sposób zarządzania**   * zdalny dostęp pozwalający administratorom na wdrażanie, monitorowanie, konfigurowanie i aktualizowanie serwerów * dedykowany port do komunikacji z siecią * zarządzanie za pomocą poleceń interfejsu IPMI, DCMI, Racadm, a także za pomocą interfejsu graficznego * monitoring wszystkich kluczowych komponentów (wentylatory, zasilacze, pamięć, procesor, RAID, karty sieciowe oraz dyski twarde) * informacje o aktualnym zużyciu energii oraz temperaturach * kontrola zasilania (włączenie, wyłączenie, restart * podstawowe funkcje diagnostyczne: podgląd dziennika systemowego, dziennika kontrolera cyklu życia * odtworzenie konfiguracji sprzętowej na podstawie kopii z innego serwera * możliwość skonfigurowania wielu kont  o zróżnicowanym poziomie przywilejów (wg na ról) * szyfrowanie protokołem SSL * powiadomienia e-mail * możliwość blokowania adresów IP * generowanie wykresów oraz konfigurowanie progów i alertów | \* |
|  | **Diagnostyka**  Panel umieszczony na froncie obudowy, umożliwiający wyświetlenie, stan procesora, pamięci, dysków oraz pozostałych komponentów płyty głównej. | \* |
|  | **Wymagania dodatkowe:**   * Obudowa trwale oznaczona opisem technicznych detali zawierająca przynajmniej informacje o zainstalowanym procesorze, pamięci operacyjnej, typie systemu. | \* |
|  | **Certyfikaty**  Serwer musi być wyprodukowany zgodnie z normą ISO-7779 oraz ISO-9296 Deklaracja CE | \* |
|  | **Dokumentacja użytkownika**  Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. | \* |
| 1. **WARUNKI GWARANCJI, NAPRAW, SERWIS itp.** | | |
|  | GwarancjaNBD z zachowaniem dysków twardych przypadku awarii.  Gwarancja liczona od dnia protokolarnego odbioru przedmiotu zamówienia przez Zamawiającego | \* |
|  | Okres gwarancji w przypadku wymiany przedmiotu zamówienia na nowy:  taki jak oferowany w ofercie, liczony od momentu wymiany przedmiotu zamówienia na nowy | \* |
|  | Czas reakcji na zgłoszenie awarii = przyjazd serwisanta do Zamawiającego:  do **24h** od momentu zgłoszenia telefonicznego | \* |
|  | Miejsce wykonania naprawy  w pierwszej kolejności u Zamawiającego, jeżeli nie jest to możliwe w serwisie autoryzowanym Wykonawcy | \* |
|  | Maksymalny czas naprawy przedmiotu zamówienia w przypadku kiedy naprawa wykonywana jest w siedzibie Zamawiającego: **max 48 h** | \* |
|  | Maksymalny czas naprawy przedmiotu zamówienia w przypadku kiedy naprawa wykonywana jest w siedzibie autoryzowanego serwisu Wykonawcy: **max 14 dni** | \* |
|  | Na czas naprawy przedmiotu zamówienia wykonywanej w serwisie autoryzowanym Wykonawcy Wykonawca zobowiązuje się do dostarczenia urządzenia zastępczego | \* |
|  | Przedłużenie okresu gwarancji o czas wyłączenia z eksploatacji przedmiotu zamówienia **po max 14 dniach** | \* |
|  | W okresie gwarancji w przypadku konieczności naprawy przedmiotu zamówienia w serwisie autoryzowanym Wykonawcy, koszt ewentualnego transportu do i z serwisu pokrywa Wykonawca | \* |
|  | Magazyn części zamiennych  dostępność oryginalnych części zamiennych przez okres min. 2 lat po upływie gwarancji | \* |
|  | Dane serwisanta uprawnionego do odebrania i przyjęcia do realizacji ewentualnych zgłoszeń / awarii przedmiotu zamówienia | Osoba do kontaktu:  ……………………………………….  Imię i nazwisko  Telefon: ………………………………………..…………  Mail: …………………………………………….….…. |
|  | Bezpłatny serwis gwarancyjny | Nazwa:  …………………………………………………..  Adres:  …………………………………………………..  Nr telefonu:  …………………………………………………... |

\* ***wypełnia Wykonawca***

…………….……. *(miejscowość),*dnia ………….……. r.

...........................................................................................

Własnoręczny podpis/y i pieczęć osoby/osób uprawnionej/ uprawnionych do reprezentowania wykonawcy

**Załącznik Nr 2 do SIWZ**

Dostawa serwera typ 2 - ilość: 2 szt.

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Producent : ………………………………………..

Nazwa lub model: ..………………………………………

**Rok produkcji: 2018**

|  |  |  |
| --- | --- | --- |
| Lp. | **OPIS** | **PARAMETRY OFEROWANE - opisać, wypełnić\*** |
| 1. **PARAMETRY WYMAGANE** | | |
|  | **Obudowa**  Obudowa w rozmiarze 2U przystosowana do montażu w szafie rack19”, wyposażona w teleskopowe szyny montażowe i prowadnice kabli, umożliwiająca instalacje min. 8 HDD | \* |
|  | **Płyta główna**  Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Przystosowana do pracy z procesorami serwerowymi. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. | \* |
| 3. | **Chipset**  Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych | \* |
| 4. | **Procesor**  **2 procesory16 rdzeniowe** z taktowaniem zegara 2.10GHz osiągające w teście wydajności PassMarkAverage CPU Mark co najmniej 19 100 punktów – każdy pracujący w architekturze 64 bit przystosowane do pracy w środowisku o wysokim współczynniku obciążenia i zapotrzebowania na zasoby obliczeniowe. Procesory musz**ą** obsługiwać wszystkie, aktualnie dostępne technologie wirtualizacyjne, opracowane przez producenta danego procesora.  Wynik testu dostępny pod adresem <https://www.cpubenchmark.net>  Zamawiający zastrzega sobie prawo do dokonanie weryfikacji parametrów oferowanego procesora na dzień otwarcia ofert poprzez wydrukowanie ze strony <https://www.cpubenchmark.net> testu wydajności.  W przypadku uzyskania w teście wydajności na dzień otwarcia ofert wartości niższych niż oferowane **oferta będzie podlegała odrzuceniu.** | \*Podać wydajność procesora:  …………………………………. |
| 5. | **RAM**  Nie mniej niż**128GB**, Wymagane jest zaoferowanie najszybszej (dla oferowanego modelu serwera) wersji pamięci operacyjnej dostępnej w ofercie producenta oferowanego serwera i w pełni kompatybilnej z zaoferowanym procesorem. | \*Podać pojemność:  ……………………………………….. |
| 6. | **Interfejsy sieciowe**  4 porty RJ-45 GbE | \* |
| 7. | **Napęd optyczny**  Wewnętrzny napęd DVD+/-RW | \* |
| **8.** | **Dyski twarde**  Możliwość instalacji dysków SATA, SAS oraz SSD 3,5‘‘. Zainstalowane, co najmniej 4 dyski twarde:   * 2 x 400GB SSD, * 2x 900GB SAS 15k | \* |
| 9. | **Kontroler RAID**   * Typ kontrolera: Sprzętowy, * Poziomy RAID 0,1,5,6,10,50,60 * Rodzaje dysków SATA, SAS, SSD, SED * Pamięć cache 2GB NV * Max. transfer 12Gb/s | \* |
| 10. | **Porty**   * 4 x USB * VGA, * 1 port szeregowy (RS – 232-C) | \* |
| 11. | **Video**  Zintegrowana karta graficzna. wyście D-SUB | \* |
| 12. | **Zasilacze**  Dwa niezależne źródła zasilania 750W; redundantne – zdolne do obsługi awarii jednego źródła zasilania przy ciągłym dostarczeniu mocy niezbędnej do zasilenia serwera | \* |
| 13. | **Bezpieczeństwo**  Zintegrowany z płytą główną moduł TPM | \* |
| 14. | **Zarządzanie**  Dedykowany moduł zdalnego zarządzania, diagnostyki  i monitorowania pracy serwera. **Zarządzanie realizowane poprzez dedykowany port** | Podać czas pracy:  ……………………………………….. |
| 15. | **Sposób zarządzania**   * wdrażanie, monitorowanie, konfigurowanie i aktualizowanie serwerów * dedykowanyportdo komunikacji z siecią * zarządzanie za pomocą poleceń interfejsu IPMI, DCMI, Racadm, a także za pomocą interfejsu graficznego * monitoring wszystkich kluczowych komponentów (wentylatory, zasilacze, pamięć, procesor, RAID, karty sieciowe oraz dyski twarde) * informacje o aktualnym zużyciu energii oraz temperaturach * kontrola zasilania (włączenie, wyłączenie, restart * podstawowe funkcje diagnostyczne: podgląd dziennika systemowego, dziennika kontrolera cyklu życia * odtworzenie konfiguracji sprzętowej na podstawie kopii z innego serwera * możliwość skonfigurowania wielu kont o zróżnicowanym poziomie przywilejów (wg na ról) * szyfrowanie protokołem SSL * powiadomienia e-mail * możliwość blokowania adresów IP * generowanie wykresów oraz konfigurowanie progów i alertów | \* |
| 16. | **Diagnostyka**  Panel umieszczony na froncie obudowy, umożliwiający wyświetlenie, stanie procesora, pamięci, dysków oraz pozostałych komponentów płyty głównej | \* |
| 17. | **Wymagania dodatkowe:**   * Obudowa trwale oznaczona opisem technicznych detali zawierająca przynajmniej informacje o zainstalowanym procesorze, pamięci operacyjnej, typie systemu | \* |
| 18. | **System operacyjny**  Microsoft Windows Server 2016 Standard 16 Core | \* |
| 19. | **Certyfikaty**  Serwer musi być wyprodukowany zgodnie z normą ISO-7779 oraz ISO-9296 Deklaracja CE  **Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać minimum status „Supported” dla MS Windows Server 2016 w wersjach x86 i x64.** | \* |
| 20. | **Dokumentacja użytkownika**  Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. | \* |
| 1. **WARUNKI GWARANCJI, NAPRAW, SERWIS itp.** | | |
| 1. | GwarancjaNBD z zachowaniem dysków twardych przypadku awarii.  Gwarancja liczona od dnia protokolarnego odbioru przedmiotu zamówienia przez Zamawiającego | \* |
| 2. | Wymiana elementu/podzespołu na nowy w przypadku braku możliwości naprawy elementu/podzespołu lub dwukrotnej naprawy tego samego elementu/podzespołu | \* |
| 3. | Okres gwarancji w przypadku wymiany przedmiotu zamówienia na nowy:  taki jak oferowany w ofercie, liczony od momentu wymiany przedmiotu zamówienia na nowy | \* |
| 4. | Czas reakcji na zgłoszenie awarii = przyjazd serwisanta do Zamawiającego:  do **24h** od momentu zgłoszenia telefonicznego | \* |
| 5. | Miejsce wykonania naprawy  w pierwszej kolejności u Zamawiającego, jeżeli nie jest to możliwe w serwisie autoryzowanym Wykonawcy | \* |
| 6. | Maksymalny czas naprawy przedmiotu zamówienia w przypadku kiedy naprawa wykonywana jest w siedzibie Zamawiającego: **max 48 h** | \* |
| 7. | Maksymalny czas naprawy przedmiotu zamówienia w przypadku kiedy naprawa wykonywana jest w siedzibie autoryzowanego serwisu Wykonawcy: **max 14 dni** | \* |
| 8. | Na czas naprawy przedmiotu zamówienia wykonywanej w serwisie autoryzowanym Wykonawcy Wykonawca zobowiązuje się do dostarczenia urządzenia zastępczego | \* |
| 9. | Przedłużenie okresu gwarancji o czas wyłączenia z eksploatacji przedmiotu zamówienia **po max 14 dniach** | \* |
| 10. | W okresie gwarancji w przypadku konieczności naprawy przedmiotu zamówienia w serwisie autoryzowanym Wykonawcy, koszt ewentualnego transportu do i z serwisu pokrywa Wykonawca | \* |
| 11. | Magazyn części zamiennych  dostępność oryginalnych części zamiennych przez okres min. 2 lat po upływie gwarancji | \* |
| 12. | Dane serwisanta uprawnionego do odebrania i przyjęcia do realizacji ewentualnych zgłoszeń / awarii przedmiotu zamówienia | Osoba do kontaktu:  ……………………………………….  Imię i nazwisko  Telefon: ………………………………………..…………  Mail: …………………………………………….….…. |
| 13. | Bezpłatny serwis gwarancyjny | Nazwa:  …………………………………………………..  Adres:  …………………………………………………..  Nr telefonu:  …………………………………………………... |

\* ***wypełnia Wykonawca***

…………….……. *(miejscowość),*dnia ………….……. r.

...........................................................................................

Własnoręczny podpis/y i pieczęć osoby/osób uprawnionej/ uprawnionych do reprezentowania wykonawcy

**Załącznik Nr 3 do SIWZ**

Dostawa serwera plików- ilość: 2 szt.

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Producent : ………………………………………..

Nazwa lub model: ..………………………………………

**Rok produkcji: 2018**

|  |  |  |
| --- | --- | --- |
| Lp. | **OPIS** | **PARAMETRY OFEROWANE - opisać, wypełnić\*** |
| 1. **PARAMETRY WYMAGANE** | | |
| 1. | **Obudowa**  Obudowa w rozmiarze 3U przystosowana do montażu w szafie rack19”, wyposażona w teleskopowe szyny montażowe i prowadnice kabli. | \* |
| 2. | **Przechowywanie**   * kieszeń/kieszenie na dyski **min.12** * obsługa dysków **2.5" SATA HDD, 2.5" SATA SSD, 3.5" SATA HDD** * Maksymalna pojemność 96TB   Obsługa hot-swap | \* |
| 3. | **Porty**   * 4 x RJ-45 1GbE 4 *(z obsługą funkcji Link Aggregation / przełączania awaryjnego)* * 2 x USB 3.0 * 2 x USB 2.0 * 2 x Gniazda rozszerzenia | \* |
| 4. | **Procesor**  Procesor czterordzeniowy, osiągający w teście wydajności PassMarkAverage CPU Mark co najmniej 9700 punktów  *wynik dostępny pod adresem* [*https://www.cpubenchmark.net*](https://www.cpubenchmark.net)  Zamawiający zastrzega sobie prawo do dokonanie weryfikacji parametrów oferowanego procesora na dzień otwarcia ofert poprzez wydrukowanie ze strony <https://www.cpubenchmark.net> testu wydajności.  W przypadku uzyskania w teście wydajności na dzień otwarcia ofert wartości niższych niż oferowane **oferta będzie podlegała odrzuceniu.** | \*Podać wydajność procesora:  …………………………………. |
| 5. | **RAM**  Nie mniej niż **16GB**, z możliwością rozbudowy do 64GB | \*Podać pojemność:  ……………………………………….. |
| 6. | **System operacyjny - funkcje**   * Wbudowany serwer: CIFS/SMB, FTP, NFS, * Integracja z Microsoft Active Directory (AD) i LDAP * Możliwość zwiększania rozmiarów wolumenów bez konieczności wyłączania dostępu do nich (online), * Dwustopniowe uwierzytelnianie użytkowników * Obsługa High Availability * Szyfrowanie AES z kluczem 256-bitowym * Automatyczne blokowanie adresów IP | \* |
| 7. | **Dyski twarde**  Zainstalowane, co najmniej:   * 4 x SATA 4TB HGST NAS * 2 x SSD 500GB SATA | \* |
| 8. | **Kontroler RAID**   * RAID 0 * RAID 1 * RAID 5 * RAID 6 * RAID 10 | \* |
| 9. | **Dokumentacja użytkownika**  Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. | \* |
| 10. | **Zarządzanie**  Dostęp do zarządzania poprzez HTTPS i SSH | \* |
| 1. **WARUNKI GWARANCJI, NAPRAW, SERWIS itp.** | | |
| 1. | Gwarancja liczona od dnia protokolarnego odbioru przedmiotu zamówienia przez Zamawiającego | \* |
| 2. | Wymiana elementu/podzespołu na nowy w przypadku braku możliwości naprawy elementu/podzespołu lub dwukrotnej naprawy tego samego elementu/podzespołu | \* |
| 3. | Okres gwarancji w przypadku wymiany przedmiotu zamówienia na nowy:  taki jak oferowany w ofercie, liczony od momentu wymiany przedmiotu zamówienia na nowy | \* |
| 4. | Czas reakcji na zgłoszenie awarii = przyjazd serwisanta do Zamawiającego:  do **24h** od momentu zgłoszenia telefonicznego | \* |
| 5. | Miejsce wykonania naprawy  w pierwszej kolejności u Zamawiającego, jeżeli nie jest to możliwe w serwisie autoryzowanym Wykonawcy | \* |
| 6. | Maksymalny czas naprawy przedmiotu zamówienia w przypadku kiedy naprawa wykonywana jest w siedzibie Zamawiającego: **max 48 h** | \* |
| 7. | Maksymalny czas naprawy przedmiotu zamówienia w przypadku kiedy naprawa wykonywana jest w siedzibie autoryzowanego serwisu Wykonawcy: **max 14 dni** | \* |
| 8. | Na czas naprawy przedmiotu zamówienia wykonywanej w serwisie autoryzowanym Wykonawcy Wykonawca zobowiązuje się do dostarczenia urządzenia zastępczego | \* |
| 9. | Przedłużenie okresu gwarancji o czas wyłączenia z eksploatacji przedmiotu zamówienia **po max 14 dniach** | \* |
| 10. | W okresie gwarancji w przypadku konieczności naprawy przedmiotu zamówienia w serwisie autoryzowanym Wykonawcy, koszt ewentualnego transportu do i z serwisu pokrywa Wykonawca | \* |
| 11. | Magazyn części zamiennych  dostępność oryginalnych części zamiennych przez okres min. 2 lat po upływie gwarancji | \* |
| 12. | Dane serwisanta uprawnionego do odebrania i przyjęcia do realizacji ewentualnych zgłoszeń / awarii przedmiotu zamówienia | Osoba do kontaktu:  ……………………………………….  Imię i nazwisko  Telefon: ………………………………………..…………  Mail: …………………………………………….….…. |
| 13. | Bezpłatny serwis gwarancyjny | Nazwa:  …………………………………………………..  Adres:  …………………………………………………..  Nr telefonu:  …………………………………………………... |

\* ***wypełnia Wykonawca***

…………….……. *(miejscowość),*dnia ………….……. r.

...........................................................................................

Własnoręczny podpis/y i pieczęć osoby/osób uprawnionej/ uprawnionych do reprezentowania wykonawcy

**Załącznik Nr 4 do SIWZ**

Dostawa zintegrowanego systemu bezpieczeństwa sieci z urządzeniem UTM

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Producent : ………………………………………..

Nazwa lub model: ..………………………………………

**Rok produkcji: 2018**

|  |  |  |
| --- | --- | --- |
| Lp. | **OPIS** | **PARAMETRY OFEROWANE - opisać, wypełnić\*** |
| 1. **PARAMETRY WYMAGANE** | | |
| 1. | **Zastosowanie**  Zintegrowany system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza | \* |
| 2. | **Monitoring i wykrywanie awarii**   * dla funkcji: 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. * Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. * monitoring stanu realizowanych połączeń VPN. * System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. | \* |
| 3. | **Parametry wydajnościowe**   * W zakresie Firewall’a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 135.000 nowych połączeń na sekundę. * Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 512 B. * Przepustowość Stateful Firewall: nie mniej niż 9 Gbps dla pakietów 64 B. * Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.5 Gbps. * Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 9 Gbps. * Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu HTTP - minimum 6 Gbps. * Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.2 Gbps. * Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 1 Gbps. | \* |
| 4. | **Funkcje Systemu Bezpieczeństwa**   * Kontrola dostępu - zapora ogniowa klasy StatefulInspection. * 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 - IntrusionPrevention System. * Kontrola stron WWW. * Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. * Zarządzanie pasmem (QoS, Trafficshaping). * Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). * Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. * Analiza ruchu szyfrowanego protokołem SSL. * Analiza ruchu szyfrowanego protokołem SSH. | \* |
| 5. | **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) dlaprotokołu SIP. * W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. | \* |
| 6. | **Interfejsy, Dysk, Zasilanie**   * System realizujący funkcję Firewall musi dysponować minimum: * 18 portami Gigabit Ethernet RJ-45. * 4 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. * System musi być wyposażony w zasilanie AC. | \* |
| 7. | **Połączenia VPN**   1. 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/CounterMode(GCM) * Obsługa protokołu Diffie-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.  1. 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. | \* |
| 8. | **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. | \* |
| 9. | **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 | \* |
| 10. | **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. | \* |
| 11. | **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 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 * Wykrywanie i blokowanie komunikacji C&C do sieci botnet | \* |
| 12. | **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 * Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur | \* |
| 13. | **Kontrola 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 (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxyavoidance * 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. | \* |
| 14. | **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 | \* |
| 15. | **Zarządzenie**   * 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, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. | \* |
| 16. | **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 | \* |
| 17. | **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 IPSec VPN * ICSA dla funkcji SSL VPN | \* |
| 18 | **Serwisy i licencje**  Wraz z dostawą urządzenia sieciowego UTM Wykonawca udzieli 36 miesięcznej licencji na przedmiot umowy w zakresie wsparcia oraz wszystkich znanych pól eksploatacji upoważniającej do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować min:   1. Kontrola Aplikacji; 2. IPS, Antywirus; 3. Antyspam; 4. Web Filtering | \* |
| 1. **WARUNKI GWARANCJI, NAPRAW, SERWIS** | | |
| 1. | Gwarancja liczona od dnia protokolarnego odbioru jakościowego przedmiotu zamówienia przez Zamawiającego | \* |
| 2. | Wymiana elementu/podzespołu na nowy w przypadku braku możliwości naprawy elementu/podzespołu lub dwukrotnej naprawy tego samego elementu/podzespołu | \* |
| 3 | Wsparcie techniczne w godzinach pracy Zamawiającego w tym celu Wykonawca powinien dysponować minimum trzema inżynierami posiadającymi certyfikat potwierdzający odpowiednie kwalifikacje z zakresu instalacji, konfiguracji i rozwiązywania problemów dotyczących wszystkich funkcjonalności i możliwości zaoferowanego urządzenia. | \* |
| 4. | Okres gwarancji w przypadku wymiany przedmiotu zamówienia na nowy:  taki jak oferowany w ofercie, liczony od momentu wymiany przedmiotu zamówienia na nowy | \* |
| 5. | Czas reakcji na zgłoszenie awarii = przyjazd serwisanta do Zamawiającego:  do **24h** od momentu zgłoszenia telefonicznego | \* |
| 6. | Miejsce wykonania naprawy  w pierwszej kolejności u Zamawiającego, jeżeli nie jest to możliwe w serwisie autoryzowanym Wykonawcy | \* |
| 7. | Maksymalny czas naprawy przedmiotu zamówienia w przypadku kiedy naprawa wykonywana jest w siedzibie Zamawiającego: **max 48 h** | \* |
| 8. | Maksymalny czas naprawy przedmiotu zamówienia w przypadku kiedy naprawa wykonywana jest w siedzibie autoryzowanego serwisu Wykonawcy: **max 14 dni** | \* |
| 9. | Na czas naprawy przedmiotu zamówienia wykonywanej w serwisie autoryzowanym Wykonawcy Wykonawca zobowiązuje się do dostarczenia urządzenia zastępczego | \* |
| 10. | Przedłużenie okresu gwarancji o czas wyłączenia z eksploatacji przedmiotu zamówienia **po max 14 dniach** | \* |
| 11. | W okresie gwarancji w przypadku konieczności naprawy przedmiotu zamówienia w serwisie autoryzowanym Wykonawcy, koszt ewentualnego transportu do i z serwisu pokrywa Wykonawca | \* |
| 12. | Magazyn części zamiennych  dostępność oryginalnych części zamiennych przez okres min. 2 lat po upływie gwarancji | \* |
| 13. | Dane serwisanta uprawnionego do odebrania i przyjęcia do realizacji ewentualnych zgłoszeń / awarii przedmiotu zamówienia | Osoba do kontaktu:  ……………………………………….  Imię i nazwisko  Telefon: ………………………………………..…………  Mail: …………………………………………….….…. |
| 14. | Bezpłatny autoryzowany serwis gwarancyjny | Nazwa:  …………………………………………………..  Adres:  …………………………………………………..  Nr telefonu:  …………………………………………………... |
| **SZKOLENIE** | | |
| 1. | Bezpłatne szkolenie w zakresie obsługi i zaawansowanej konfiguracji dostarczonego urządzenia (m.in. obejmujące zakres konfiguracji, definiowania polityk zapory, filtrowania poczty, skanowania antywirusowego, filtrowania stron Web, kontroli aplikacji, konfiguracji VPN, logowania i alertów, generowania raportów, wykrywania nieprawidłowości) zostanie przeprowadzone dla trzech pracowników wyznaczonych przez Zamawiającego (szkolenie co najmniej 8 h).  Termin szkolenia: do 21 dni od dnia dostawy.  Po zakończeniu bezpłatnego szkolenia Zamawiający otrzyma dokument potwierdzający jego odbycie w postaci certyfikatu lub zaświadczenia.  Miejsce szkolenia:siedziba Zamawiającego.  Zamawiający dopuszcza możliwość przeprowadzenia szkolenia poza siedzibą Zamawiającego za jego wcześniejszą zgodą pod warunkiem że odbędzie się ono na terenie Katowic. | |

\* ***wypełnia Wykonawca***

…………….……. *(miejscowość),*dnia ………….……. r.

...........................................................................................

Własnoręczny podpis/y i pieczęć osoby/osób uprawnionej/ uprawnionych do reprezentowania wykonawcy

**Załącznik nr 5 do SIWZ**

Miejscowość ………………. dnia ……………….

…………………………………………

Pieczęć firmowa wykonawcy

**OFERTA**

**DLA SAMODZIELNEGO PUBLICZNGO SZPITALA KLINICZNEGO**

**IM. ANDRZEJA MIELĘCKIEGO ŚLĄSKIEGO UNIWERSYTETU MEDYCZNEGO**

**W KATOWICACH**

Nazwa wykonawcy: …………………………………………................................…………………………………

Siedziba: ……………………………………………………………....................................……………

REGON: ……………………………….............. NIP:……………………………….................

Tel: . ………………………………..............… Fax: ………………………………..............…

Osoba upoważniona do kontaktu z zamawiającym:

…………………………………………………………………………………………………

Tel: . ………………………………..............… e-mail:**………………………………………………..**

Osoba upoważniona do podpisania umowy:

………………………………………………………………………….

***Zamawiający wymaga wypełnienia wszystkich pól / podania wszystkich danych wymaganych w ramce powyżej***

W nawiązaniu do ogłoszenia o przetargu nieograniczonymoferuję wykonanie dostawy na warunkach określonych w specyfikacji istotnych warunków zamówienia za cenę:

## Pakiet nr 1 - Dostawa serwera typ 1

Cena bez podatku VAT za 1 szt. ………………...……………….…..… zł

podatek VAT ………% …………………….………….………………… zł

**Cena ofertowa z podatkiem VAT za 1szt.** .………………….……… zł

Słownie: …………………………..………………………………………………………………………...........zł

**OKRES GWARANCJI:** ……………..**miesięcy\***

**TERMIN DOSTAWY: ……………..dni\***

***\*kryterium ocenne***

## Pakiet nr 2 - Dostawa serwera typ 2

Cena bez podatku VAT za 2 szt. ………………...……………….…..… zł

podatek VAT ………% …………………….………….………………… zł

**Cena ofertowa z podatkiem VAT za 2 szt.** .………………….……… zł

Słownie: …………………………..………………………………………………………………………...........zł

**OKRES GWARANCJI:** ……………..**miesięcy\***

**TERMIN DOSTAWY: ……………..dni\***

***\*kryterium ocenne***

## Pakiet nr 3 - Dostawa serwera NAS

Cena bez podatku VAT za 2 szt. ………………...……………….…..… zł

podatek VAT ………% …………………….………….………………… zł

**Cena ofertowa z podatkiem VAT za 2 szt.** .………………….……… zł

Słownie: …………………………..………………………………………………………………………...........zł

**OKRES GWARANCJI:** ……………..**miesięcy\***

**TERMIN DOSTAWY: ……………..dni\***

***\*kryterium ocenne***

## Pakiet nr 4 - Dostawa i wdrożenie zintegrowanego systemu bezpieczeństwa z urządzeniem UTM

Cena bez podatku VAT ..………………...……………….…..… zł

podatek VAT ………% ………….………….………………… zł

**Cena ofertowa z podatkiem VAT …….**.………………….……… zł

Słownie: …………………………..………………………………………………………………………...........zł

**OKRES GWARANCJI:** ……………..**miesięcy\***

**TERMIN DOSTAWY: ……………..dni\***

***\*kryterium ocenne***

1. Oświadczamy, że cena/y brutto zawarta/e w Ofercie zawierają wszystkie koszty, jakie ponosi Zamawiający w przypadku wyboru niniejszej oferty.
2. Oświadczamy, że akceptujemy warunki płatności określone przez Zamawiającego   
   w Specyfikacji Istotnych Warunków Zamówienia przedmiotowego postępowania.
3. Oświadczamy, że jesteśmy związani niniejszą ofertą przez okres 30 dni od dnia upływu terminu składania ofert.
4. Oświadczamy, że niniejsza oferta zawiera na stronach nr od \_\_\_\_ do \_\_\_\_ informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.
5. Oświadczamy, że zapoznaliśmy się z projektem umowy, stanowiącym załącznikdo Specyfikacji Istotnych Warunków Zamówienia i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy zgodnej z niniejszą ofertą, na warunkach określonych w Specyfikacji Istotnych Warunków Zamówienia, w miejscu i terminie wyznaczonym przez Zamawiającego
6. Ofertę niniejszą składam na \_\_\_\_\_\_\_\_\_ kolejno ponumerowanych stronach.

…………….……. *(miejscowość),* dnia ………….……. r.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Własnoręczny podpis osoby/osób uprawnionej/uprawnionych*

*do reprezentowania Wykonawcy*

**ZAŁĄCZNIK NR 6 do SIWZ**

***Zamawiający:***

**SP Szpital Kliniczny im. Andrzeja Mielęckiego**

**Śląskiego Uniwersytetu Medycznego w Katowicach**

**40-027 Katowic ul. Francuska 20/24**

***Wykonawca:***

………………………………………………

……………………………..………………

*(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

***reprezentowany przez:***

………………………………………………

……………………..………………………

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

**Oświadczenie wykonawcy**

**składane na podstawie art. 25a ust. 1 ustawy z dnia 29 stycznia 2004 r.**

**Prawo zamówień publicznych (dalej jako: ustawa Pzp),**

**DOTYCZĄCE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **DOSTAWA SERWERÓW ORAZ DOSTAWA I WROŻENIE ZINTEGROWANEGO SYSTEMU BEZPIECZEŃSTWA SIECI Z URZĄDZENIEM UTM**, prowadzonego przez SPSKM w Katowicach*,*oświadczam, co następuje:

**INFORMACJA DOTYCZĄCA WYKONAWCY:**

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez zamawiającego w SIWZ w postępowaniu o udzielenie zamówienia publicznego.

…………….……. *(miejscowość),*dnia ………….……. r.

…………………………………………

*Własnoręczny podpis osoby/osób uprawnionej/uprawnionych*

*do reprezentowania Wykonawcy*

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. …………. ustawy Pzp*(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 24 ust. 1 pkt 13-14, 16-20 lub art. 24 ust. 5 ustawy Pzp).*Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 24 ust. 8 ustawy Pzp podjąłem następujące środki naprawcze:

……………………………………………………………………………………………………………………

…………………………………………………………………………………………..…………………...........………..……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(miejscowość),* dnia \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ r.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Własnoręczny podpis osoby/osób uprawnionej/uprawnionych*

*do reprezentowania Wykonawcy*

**ZAŁĄCZNIK NR 7 do SIWZ**

**Zamawiający:**

**SP Szpital Kliniczny im. Andrzeja Mielęckiego**

**Śląskiego Uniwersytetu Medycznego w Katowicach**

**40-027 Katowic ul. Francuska 20/24**

**Wykonawca:**

………………………………………………………………………………

*(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

reprezentowany przez:

………………………………………………………………………………………………

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

**Oświadczenie wykonawcy**

**składane na podstawie art. 24 ust. 11 ustawy z dnia 29 stycznia 2004 r.**

**Prawo zamówień publicznych (dalej jako: ustawa Pzp),**

**DOTYCZĄCE PRZYNALEŻNOŚCI DO GRUPY KAPITAŁOWEJ**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **DOSTAWA SERWERÓW ORAZ DOSTAWA I WROŻENIE ZINTEGROWANEGO SYSTEMU BEZPIECZEŃSTWA SIECI Z URZĄDZENIEM UTM** prowadzonego przez SPSKM w Katowicach*,* oświadczam, co następuje:

Składając ofertę w postępowaniu o udzielnie zamówienia publicznego w zakresie **Pakietu nr ……..,** prowadzonym przez SPSKM Katowice oświadczamy, że:

1. nie należymy do grupy kapitałowej, o której mowa w art. 24 ust. 11 ustawy Prawo zamówień publicznych \*,
2. należymy do grupy kapitałowej, o której mowa w art. 24 ust. 11 ustawy Prawo zamówień publicznych\*. W przypadku przynależności Wykonawcy do grupy kapitałowej, o której mowa w art. 24 ust. 11 ustawy Prawo zamówień publicznych, Wykonawca składa wraz z ofertą listę podmiotów należących do grupy kapitałowej.

…………….……. *(miejscowość),*dnia ………….……. r.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Własnoręczny podpis osoby/osób uprawnionej/uprawnionych*

*do reprezentowania Wykonawcy*

\* - niepotrzebne skreślić.

**\*** *należy zaznaczyć właściwą odpowiedź***;** *wykonawca, który należy do grupy kapitałowej zobowiązany jest do złożenia listy podmiotów należących do tej samej grupy kapitałowej*