**ZMIANA SIWZ Z DNIA 25.01.2021r.**

**Załącznik Nr 2 do SIWZ**

**….…….……………………..**

nazwa i adres Wykonawcy

**pieczęć firmowa**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**- OFERTA CENOWA**

**Pakiet 1**

|  |  |  |  |
| --- | --- | --- | --- |
| **Serwery wirtualizacji z gwarancją w ilości 4 kpl.**  Nazwa sprzętu: ………………………………………  Model/Symbol: ………………………………………  Producent: …………………………………………...  Rok produkcji: **……….** ( sprzęt fabrycznie nowy, nieużywany ) | | | |
| **Typ** | **Parametry techniczne** | **Minimalne**  **parametry wymagane/**  **punktowane**  **parametry** | **Parametry oferowane**  **(należy potwierdzić TAK/NIE)** |
| **Obudowa:** | Obudowa Rack o wysokości max 2U z możliwością instalacji co najmniej 4 dysków 2,5" HotPlug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem kabli. Zintegrowany z płytą główną moduł TPM. | TAK |  |
| Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą | 10 PKT. |  |
| **Płyta główna** | Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. | TAK |  |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. | TAK |  |
| **Procesor** | Zainstalowane dwa procesory min. 16-rdzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 168 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. | TAK | …………….  …………….  (należy podać) |
| **Pamięć RAM** | DIMM DDR4 512GB ECC, po wypełnieniu slotów płyty wymaganą ilością pamięci, powinna pozostać możliwość dodania co najmniej kolejnych 512GB | TAK |  |
| **Funkcjonalność pamięci RAM** | Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling | TAK |  |
| **Gniazda PCI** | Minimum trzy sloty PCIe x16 generacji 3 | TAK |  |
| **Kontroler RAID** | 1. Sprzętowy kontroler dyskowy posiadający min. 2GB **nieulotnej** pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. | 2 PKT. |  |
| 2. Dopuszcza się sprzętowy kontroler dyskowy posiadający min. 2GB pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. | 0 PKT. |  |
| **Dyski i Napędy** | 2 dyski SSD SAS lub NVMe lub HDD SAS 10krpm o pojemność co najmniej 100GB skonfigurowane w RAID1. | TAK |  |
| **Karta sieciowe** | 8 portów 10Gbps SFP+ - jeżeli część portów będzie w formie zintegrowanej z płytą, a część poprzez kartę rozszerzeń, wszystkie muszą być takie same i umożliwić bezproblemowe tworzenie zagregowanych połączeń Link Aggregation według IEEE 802.1AX-2008 pod kontrolą zainstalowanego systemu operacyjnego serwera. Wszystkie porty muszą być wyposażone w moduły optyczne o parametrach:   * złącze LC Duplex * transmisja na odległość co najmniej 300 metrów z wykorzystaniem światłowodu wielomodowego kategorii OM3 * przepustowość 10Gbps * Zgodny ze standardami: IEEE802.3Z, IEEE 802.3ae, SFP+ MSA, IEC60825 * Moduł diagnostyki cyfrowej: temperatura, napięcie zasilania, moc nadajnika, moc odbierana, prąd lasera   Długość fali 850nm | TAK |  |
| **Karty rozszerzeń** | karta FC HBA - 2 porty o łącznej przepustowości co najmniej 32Gbps wyposażone w moduły optyczne o parametrach:  typ SWL, przepustowość co najmniej 16Gbps, światłowód wielomodowy, odległość do 100 metrów przy wykorzystaniu światłowodu kategorii OM4, złącza LC Duplex | TAK |  |
| **Zdalne Zarządzanie** | Zainstalowana niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port RJ-45 Gigabit Ethernet karta umożliwiająca:  - zdalny dostęp do graficznego interfejsu Web karty zarządzającej  - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, temperaturze poszczególnych komponentów, poborze prądu, napięciach procesora, pamięci, obciążeniu poszczególnych elementów i konfiguracji serwera dla danych bieżących i historycznych co najmniej z okresu 1 tygodnia), | TAK |  |
| - możliwość konfiguracji zasobów dyskowych z poziomu interfejsu zarządzania przez przeglądarkę (utworzenia grupy RAID i wirtualnych dysków), | 20 PKT. |  |
| - monitorowanie zużycia dysków SSD w przypadku dostarczenia dysków SSD | 20 PKT. |  |
| - szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika  - możliwość podmontowania zdalnych wirtualnych napędów lub obrazów dysku w formatach obrazu ISO, RAW IMG  - wirtualną konsolę z dostępem do myszy, klawiatury  - wsparcie dla IPv6  - wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH  - integracja z Active Directory  - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej, | TAK |  |
| - Możliwość zarządzania dostarczonymi serwerami z wykorzystaniem wdrożonego u Zamawiającego oprogramowania Openmanage Enterprise, dopuszcza się realizacje poprzez dostarczenie rozwiązania o funkcjonalności opisanej poniżej jako „Oprogramowanie do zarządzania”) pod warunkiem wdrożenia dostarczonego rozwiązania i uruchomienia go dla posiadanych obecnie przez Zamawiającego urządzeń (serwery, macierze) - jeżeli spełnienie funkcjonalności wymaga dodatkowych pluginów i/lub licencji należy je dostarczyć w ramach postępowania.  Oprogramowanie do zarządzania:  Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające przynajmniej minimalne wymagania:   * wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych, * integracja z Active Directory, * wsparcie dla protokołów SNMP, IPMI, Linux SSH, * możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram, * szczegółowy opis wykrytych systemów oraz ich komponentów * możliwość eksportu raportu do CSV, HTML, XLS, PDF * możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach * szybki podgląd stanu środowiska * podsumowanie stanu dla każdego urządzenia * szczegółowy status urządzenia/elementu/komponentu * generowanie alertów przy zmianie stanu urządzenia. * filtry raportów umożliwiające podgląd najważniejszych zdarzeń * kreator umożliwiający dostosowanie akcji dla wybranych alertów * możliwość importu plików MIB * przesyłanie alertów „as-is” do innych konsol firm trzecich * możliwość definiowania ról administratorów * moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie   poszczególnych komponentów serwera.   * wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile * możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. * tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.   zdalne uruchamianie diagnostyki serwera. | 30 PKT. | ………………………………………  (należy podać) |
| **Zasilanie** | 2 redundantne zasilacze Hot-Plug, Klasa min. Platinum, sprawność min. 94% | TAK |  |
| **Wyposażenie** | Szyny ruchome z ramieniem/organizatorem na kable, komplet wkładek i patchcordów o długości 5 metrów | TAK |  |
| **Certyfikaty** | Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019. | TAK |  |
| **Gwarancja** | Gwarancja producenta świadczona przez inżyniera w miejscu instalacji sprzętu z SLA na poziomie 8x5xNBD. Możliwość zgłaszania awarii poprzez linię telefoniczną producenta lub firmy serwisującej. Możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.  Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia.  Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w  żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.  Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Firma serwisująca musi posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  Urządzenie musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający będzie wymagał dostarczenia wraz z urządzeniem oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. | TAK |  |
| **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. | TAK |  |
| **Dostarczony system operacyjny** | Zainstalowany Windows Server 2019 lub równoważny z funkcją hypervisor-a, z możliwością uruchomienia klastra pracy awaryjnej i nieograniczonej liczby maszyn wirtualnych z Windows Server na każdym z serwerów fizycznych pracujących w klastrze z systemem Windows Server na każdym z serwerów, możliwość uruchomienia w ramach dostarczonej licencji poprzednich wersji (WS2008, WS2012, WS2012R2, WS2016), możliwość uruchomienia funkcji: klastra wirtualizacji, repliki magazynu, Chronione maszyny wirtualne (VM), Software Defined Networking (SDN), Magazyn danych zdefiniowany programowo. | TAK |  |
| **I. Zakup, dostarczenie i montaż wyposażenia serwerowni tj. Pakiet 1 - Serwery wirtualizacji z uwzględnieniem 60 miesięcznej gwarancji standardowej producenta, w ilości 4 kpl. dla Katowickiego Centrum Onkologii –** zgodnie z SIWZ wraz z transportem sprzętu, przekazaniem do użytkowania, certyfikatami wraz z okresem gwarancji – zgodnym z szczegółowym opisem przedmiotu zamówienia  **Cena jedn. netto: …………………… zł**  **Cena netto za 4 kpl. = …………………………….zł**  **VAT %: ……… Kwota VAT:………..zł**  **Cena ogółem brutto: ………………………………………............** | | | |
| II. Wynik punktowy wydajności serwerów: …………….  (wynik w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej | | | |
| III. **Koszt sprzedaży ratalnej (koszt finansowania) \* w 24 równych ratach, z możliwością wcześniejszej spłaty\*\* :**  **………..…zł netto / ………….zł brutto**  \* Uwaga Należy wskazać wyłącznie koszt finansowania  \*\* Zamawiający w przypadku wcześniejszej spłaty nie będzie ponosił dodatkowych kosztów, a wartość całkowitego zobowiązania Zamawiającego będzie stanowiła wartość ceny łącznej i kosztów finansowania za poszczególne miesiące w przypadku w których Zamawiający będzie z finansowania korzystał. | | | |

UWAGA:

Wszystkie parametry wymagane stanowią kryteria, których niespełnienie spowoduje odrzucenie oferty.

**Oświadczamy**, że oferowany sprzęt jest kompletny i będzie po zainstalowaniu gotowy do pracy zgodnie z jego przeznaczeniem bez konieczności dokonania dodatkowych zakupów.

**.........................................................................................**

**data, podpis i pieczątka osoby uprawnionej**

**Załącznik Nr 2 do SIWZ**

**c.d. ….…….……………………..**

nazwa i adres Wykonawcy

**pieczęć firmowa**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**- OFERTA CENOWA**

**Pakiet 2**

|  |  |  |  |
| --- | --- | --- | --- |
| **Macierz podstawowa z gwarancją w ilości 1 kpl.**  Nazwa sprzętu: ………………………………………  Model/Symbol: ………………………………………  Producent: …………………………………………...  Rok produkcji: **……….** ( sprzęt fabrycznie nowy, nieużywany ) | | | |
| **Typ** | **Parametry techniczne** | **Mnimalne**  **parametry wymagane**  **/**  **punktowane**  **parametry** | **Parametry oferowane**  **(należy podać)** |
| **Macierz** | Macierz posiadająca dwa redundantne kontrolery macierzowe pracujące w trybie active-active wraz z możliwością instalacji co najmniej 30 dysków. | 20 PKT. |  |
| Dopuszcza się macierz posiadającą dwa redundantne kontrolery macierzowe pracujące w trybie active-active wraz z możliwością instalacji co najmniej 24 dysków. | 0 PKT. |  |
| Macierz musi umożliwiać rozbudowę o dodatkowe moduły dyskowe (poprzez dedykowane porty co najmniej 2x12 Gb SAS na każdy kontroler) przynajmniej typu:  min. 12 dysków 3,5” o wysokości do 2U,  min. 24 dysków 2,5” o wysokości do 2U,  min. 60 dysków 3,5” o wysokości do 4U.  Macierz powinna obsługiwać dyski do łącznej ilości minimum 220 dysków SAS/NLSAS lub SSD.  Macierz powinna posiadać dwa kontrolery w jednej obudowie | TAK |  |
| Całość dostarczonego rozwiązania nie może przekraczać 7U. | 5 PKT. |  |
| **Wymagana przestrzeń** | Macierz musi być wyposażona w co najmniej 10 dysków 2,5” HotPlug SSD: typu co najmniej Mix Use ( min. 3 DWPD przez 5 lat – DRIVE WRITES PER DAY) o pojemności co najmniej 1,9TB, SAS, 12Gb/s; | 5 PKT. |  |
| Dopuszcza się macierz wyposażoną w co najmniej 10 dysków 2,5” HotPlug SSD: typu co najmniej Mix Use ( min. 3 DWPD przez 5 lat – DRIVE WRITES PER DAY) o pojemności co najmniej 1,6TB, SAS, 12Gb/s; | 0 PKT. |  |
| Co najmniej 18 dysków 2,5” HotPlug SAS 12Gb o pojemności co najmniej 1.8TB, 10k rpm. | TAK |  |
| Wszystkie powyższe dyski powinny zostać zamontowane w ramach jednostki głównej macierzy. | 20 PKT. |  |
| Jeżeli jednostka główna macierzy nie umożliwia montażu wszystkich dysków, należy tak dobrać typ obudowy i półki, żeby każda z grup dysków zamontowana była w ramach jednej obudowy (kontrolerowej lub dodatkowej np. 10 dysków SSD w ramach jednostki głównej, oraz 18 dysków HDD w ramach półki dodatkowej) | TAK |  |
| Dodatkowy moduł dyskowy z możliwością zainstalowania co najmniej 60 dysków 3,5” zawierający: | TAK |  |
| 28 dysków 3,5” HotPlug o pojemności co najmniej 8TB NLSAS 12Gb/s, 7.2k rpm | TAK |  |
| **Pamięć podręczna (Cache)** | Pamięć podręczna (cache) – 128 GB pojemności użytkowej dla danych oraz informacji kontrolnych na każdy kontroler (sumarycznie 256GB). Zamawiający nie dopuszcza rozwiązań rozszerzających pamięć podręczną cache dyskami SSD/Flash. | 2 PKT. |  |
| Pamięć podręczna (cache) – 64 GB pojemności użytkowej dla danych oraz informacji kontrolnych na każdy kontroler (sumarycznie 128GB). Zamawiający nie dopuszcza rozwiązań rozszerzających pamięć podręczną cache dyskami SSD/Flash. | TAK |  |
| **Interfejsy zewnętrzne** | Wszystkie porty FC macierzy muszą być wyposażone moduły optyczne o parametrach minimalnych:  typ SWL (Short Wavelength), przepustowość 32Gbps, światłowód wielomodowy, odległość do 100 metrów przy wykorzystaniu światłowodu kategorii OM4, złącza LC Duplex | TAK |  |
| Każdy kontroler musi być wyposażony co najmniej w 4 porty FC 32Gb/s oraz 1 port zarządzający 1GbE Base-T. | TAK |  |
| Każdy kontroler musi być wyposażony w dodatkowe 4 porty FC 32Gb/s (SFP+) lub 4 porty SFP28 z wkładkami 25Gb wspierające obsługę protokołu iSCSI | 2 PKT. |  |
| **Dostępność** | Odporność na zanik zasilania jednej fazy lub awarię zasilacza macierzy (redundancja układu zasilania). Możliwość łączenia w macierzy różnych poziomów RAID:   * możliwość zastosowania RAID10 * możliwość zastosowania RAID5, * możliwość zastosowania RAID6 * możliwość zastosowania RAID0 * możliwość zastosowania RAID1   Macierz musi umożliwiać konstrukcję urządzenia LUN w taki sposób, aby zawierał dane zabezpieczone poziomami RAID 10, RAID 5, RAID 6 jednocześnie. | TAK |  |
| Macierz musi umożliwiać tworzenie kopii migawkowej (PITC) w taki sposób, aby dane były zabezpieczone innym poziomem RAID, niż dane źródłowe. (Jeżeli macierz nie umożliwia takiej funkcjonalności, należy dostarczyć dodatkowo 30% przestrzeni typu RAW) | 2 PKT. |  |
| Podwójne niezależne przyłącza SAS 12Gb/s do zewnętrznych napędów dyskowych.  Odporność na awarię pamięci cache – lustrzany zapis danych oraz technologia zapewniająca ochronę danych z pamięci cache w razie utraty zasilania.  Możliwość wykonywania wszystkich napraw, rekonfiguracji, rozbudowy i upgrade’ów (zarówno sprzętu jak i oprogramowania macierzy) w trybie online (bez przerywania pracy systemu).  Możliwość zdefiniowania min. 4 dysków zapasowych dla każdego typu dysków w zaoferowanej macierzy lub odpowiednia zapasowa przestrzeń dyskowa.  Możliwość obsługi wirtualnych portów (NPIV) w taki sposób, aby awaria fizycznego portu nie powodowała konieczności przełączania ścieżek poprzez oprogramowanie do multipathing. | TAK |  |
| **Wspierane systemy operacyjne** | Wymagane wsparcie dla różnych systemów operacyjnych, co najmniej MS Windows, VMware oraz Linux,  Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: MS Windows, Vmware, Linux.  Macierz musi mieć wsparcie dla automatycznego, bez agenta, odzyskiwania bloków (space reclamation) dla systemu operacyjnego Linux i systemu plików EXT4, NTFS dla Windows 2012, VMFSv5 dla ESX oraz VxFS w przypadku zastosowania technologii Thin Provisioning. | TAK |  |
| **Skalowalność** | Wykonywanie rozbudowy sprzętowej w trybie online.  Umożliwia rozbudowę do minimum 220 dysków 2,5”.  Możliwość rozbudowy macierzy za pomocą nowych dysków o większych pojemnościach oraz dysków typu SSD/Flash – zoptymalizowanych pod kątem zapisu bądź odczytu.  Macierz musi umożliwiać mieszanie dysków o różnych prędkościach obrotowych w ramach jednej półki dyskowej. | TAK |  |
| **Zarządzanie** | Oprogramowanie do zarządzania macierzą przez administratora klienta – graficzny interfejs do monitorowania stanu i konfiguracji macierzy, diagnostyki, mapowania zasobów do serwerów (zarówno podłączanych bezpośrednio jak i przez sieć SAN – LUN Masking).  Możliwość monitorowania wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, wolumenów logicznych LUN, oraz kontrolerów.  Wymagana możliwość zbierania i przechowywania informacji o wydajności macierzy bez ograniczeń czasowych.  Możliwość konfigurowania wolumenów logicznych LUN o pojemności użytkowej 256TB.  Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości. | TAK |  |
| Możliwość stałego monitorowania macierzy przez zdalne centrum serwisowe. | 2 PKT. |  |
| Możliwość zarządzania i monitorowania dostarczoną macierzą przez oprogramowanie opisane w Pakiecie 1 w punkcie „oprogramowanie alternatywne do zarządzania” | 5 PKT. |  |
| **Lokalna replikacja danych** | Możliwość tworzenia kopii danych z poziomu macierzy  i wewnątrz macierzy bez angażowania systemu operacyjnego hosta.  Możliwość tworzenia i utrzymywania jednocześnie minimum ośmiu lokalnych kopii danych wewnątrz macierzy dla każdego urządzenia LUN (tzw. kopie point-in-time) przez administratora.  Oferowana macierz dyskowa musi umożliwiać wykonanie lokalnej kopii danych na całej zaoferowanej przestrzeni dyskowej.  Wymaga jest również funkcjonalność wykonywania kopii wirtualnych typu snapshot. Jest wymagana licencja na pełną pojemność macierzy oraz maksymalną ilość snapshotów w obrębie macierzy.  Kopie migawkowe muszą być wykonywane metodą tzw. bez prealokacji przestrzeni dyskowej (ang. allocate-on-write, a.k.a redirect-on-write). Kopie migawkowe nie mogą być wykonywane metodą COW (ang. Copy On Write)  Kopie migawkowe muszą mieć możliwość prezentacji jako urządzenia LUN w trybie do odczytu i zapisu. Jeżeli ta funkcjonalność wymaga dodatkowej licencji należy ją dostarczyć. | TAK |  |
| **Redukcja danych** | Macierz musi zapewniać metody redukcji ilości danych blokowych za pomocą deduplikacji oraz kompresji.  Jeżeli funkcjonalność wymaga dodatkowych licencji – należy je dostarczyć. | TAK |  |
| **Kontrola przepływu danych - QoS** | Macierz dyskowa powinna posiadać mechanizmy kontroli wykorzystania zasobów macierzowych na poziomie poszczególnych woluminów. Kontrola powinna polegać na możliwości dynamicznego ograniczania przepływu danych wyrażanych w MB/s oraz w ilości IOPS poprzez administratora w dowolnym momencie.  Jeżeli funkcjonalność wymaga dodatkowych licencji – należy je dostarczyć. | TAK |  |
| **Współpraca z aplikacjami** | Możliwość integracji środowiska VMware, Microsoft SQL z mechanizmem lokalnej replikacji danych. | TAK |  |
| **Zdalna replikacja danych**  **(Zamawiający wymaga dostarczenia licencji)** | Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie synchronicznym oraz asynchronicznym i asynchronicznym interwałowym bez użycia dodatkowych serwerów lub innych urządzeń. Należy dołączyć licencję, jeśli jest wymagana.  Do replikacji wymagane jest użycie protokołu FC.  Oferowana macierz dyskowa musi umożliwiać wykonanie w trybie synchronicznym i asynchronicznym zdalnej kopii danych całej powierzchni użytkowej macierzy. | TAK |  |
| **Importowanie danych** | Macierz musi posiadać funkcjonalność online’owego importu danych z macierzy innego producenta z jednoczesną konwersją wolumenu logicznego LUN do trybu „Thin Provision” | TAK |  |
| **Gwarancja** | Gwarancja producenta świadczona przez inżyniera w miejscu instalacji sprzętu z SLA na poziomie 8x5xNBD. Możliwość zgłaszania awarii poprzez linię telefoniczną producenta lub firmy serwisującej w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.  Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia.  Minimum 5 lat usługi zapewniającej pozostawienie dysków u klienta w przypadku ich awarii.  Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia.  Urządzenie musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający będzie wymagał dostarczenia wraz z urządzeniem oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski.  Serwis świadczony przez producenta lub jego autoryzowanego przedstawiciela serwisowego.  Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Firma serwisująca musi posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. | TAK |  |
| **Wymiana dysków** | Wymiana dysków może być dokonywana przez Zamawiającego. | TAK |  |
| **Instalacja** | Cena macierzy musi zawierać usługę implementacji dla min. 8 hostów przeprowadzoną przez producenta lub autoryzowany przez producenta serwis. | TAK |  |
| **I. Zakup, dostarczenie i montaż wyposażenia serwerowni tj. Pakiet 2 - Macierz podstawowa z uwzględnieniem 60 miesięcznej gwarancji standardowej producenta w ilości 1 kpl. dla Katowickiego Centrum Onkologii –** zgodnie z SIWZ wraz z transportem sprzętu, przekazaniem do użytkowania, certyfikatami wraz z okresem gwarancji – zgodnym z szczegółowym opisem przedmiotu zamówienia  **Cena netto: …………………… zł**  **VAT %: ……… Kwota VAT:………..zł**  **Cena ogółem brutto: ………………………………………............** | | | |
| **II. Koszt sprzedaży ratalnej (koszt finansowania) \* w 24 równych ratach, z możliwością wcześniejszej spłaty\*\* :**  **………..…zł netto / ………….zł brutto**  \* Uwaga Należy wskazać wyłącznie koszt finansowania  \*\* Zamawiający w przypadku wcześniejszej spłaty nie będzie ponosił dodatkowych kosztów, a wartość całkowitego zobowiązania Zamawiającego będzie stanowiła wartość ceny łącznej i kosztów finansowania za poszczególne miesiące w przypadku w których Zamawiający będzie z finansowania korzystał. | | | |

UWAGA:

Wszystkie parametry wymagane stanowią kryteria, których niespełnienie spowoduje odrzucenie oferty.

**Oświadczamy**, że oferowany sprzęt jest kompletny i będzie po zainstalowaniu gotowy do pracy zgodnie z jego przeznaczeniem bez konieczności dokonania dodatkowych zakupów

**.........................................................................................**

**data, podpis i pieczątka osoby uprawnionej**

**Załącznik Nr 2 do SIWZ**

**….…….……………………..**

**c.d.** nazwa i adres Wykonawcy

**pieczęć firmowa**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**- OFERTA CENOWA**

**Pakiet 3**

|  |  |  |
| --- | --- | --- |
| **Przełączniki SAN (FC) z gwarancją w ilości 2 kpl.**  Nazwa sprzętu: ………………………………………  Model/Symbol: ………………………………………  Producent: …………………………………………...  Rok produkcji: **……….** ( sprzęt fabrycznie nowy, nieużywany ) | | |
| **Typ** | **Minimalne parametry wymagane** | **Parametry oferowane**  **(należy podać)** |
| **Tryby pracy przełącznika** | Switch, Access gateway |  |
| **Wspierane tryby pracy portów Fibre Channel** | E\_Ports, F\_Ports, M\_Ports, i D\_Ports |  |
| **Porty FC** | 24 porty SFP+  możliwość dowolnej kombinacji typu wkładek (Short Wavelength, Long Wavelength, Extended Long Wavelength)  zamontowane moduły wymienne w czasie pracy SFP+ 32Gbps muszą umożliwiać autonegocjację dla szybkości 8-, 16- i 32Gbps |  |
| **Zamontowane aktywowane moduły:** | w każdym z przełączników muszą być zamontowane i aktywne moduły optyczne:   * 2 moduły 32Gbps LWL na światłowód jednomodowy, wraz z patchcordami o długości 5 metrów ze złączem SC do patchpanelu i drugim zgodnym z dostarczonym modułem * 4 moduły 32Gbps SWL na światłowód wielomodowy wraz z patchcordami o długości 5 metrów ze złączami LC-LC wielomodowymi kategorii co najmniej OM4   12 modułów FC 16Gbps SWL wraz z patchcordami o długości 5 metrów ze złączami LC-LC wielomodowymi kategorii co najmniej OM4 |  |
| **Skalowalność** | Możliwość połączenia co najmniej do 20 przełączników w architekturze full-fabric |  |
| **Całkowita przepustowość** | Nie mniejsza niż 768 Gbps |  |
| **Opóźnienie** | Nie większe niż 900 ns dla urządzeń podłączonych lokalnie |  |
| **Wymagane funkcjonalności** | Traffic Isolation, QoS, port/WWN zoning, broadcast zoning, peer zoning, target-driven zoning |  |
| **ISL trunking** | obsługa do 8 portów 32Gbps na pojedynczy ISL trunk, dynamiczne równoważenie obciążenia zarówno dla pojedynczych linków w trunku, jak i dla wielu grup ISL |  |
| **Funkcje zarządzania** | Zarządzanie z wykorzystaniem: SNMP (v3), SSH i HTTPS  Możliwość przesyłania logów do zewnętrznego serwera SYSLOG  Role Based Access Control, wsparcie dla protokołu LDAP i RADIUS  Dedykowany port 10/100/1000 Mbps i szeregowy  Port USB umożliwiający upgrade firmware i pobieranie logów urządzenia |  |
| **Diagnostyka** | Wbudowana diagnostyka umożliwiająca identyfikację błędów modułów SFP, obciążenie poszczególnych portów, długość linku, monitorowanie parametrów wewnętrznych urządzenia (temperatura, zasilacz, wentylatory), FCPing, Pathinfo, flow mirroring |  |
| **Gwarancja** | Urządzenia muszą być objęte gwarancją producenta przez okres 60 miesiecy. Gwarancja realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.  Warunki gwarancji  Zamawiający wymaga, aby warunki gwarancji obejmowały w szczególności:  1) usługi w ramach gwarancji będą realizowane w siedzibie Zmawiającego,  2) czas reakcji serwisu - do końca następnego dnia roboczego od chwili zgłoszenia,  3) możliwość zgłaszania awarii w trybie 24-godzinnym przez 7 dni w tygodniu,  4)serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta,  5) gwarancja nie będzie ograniczać rekonfiguracji lub rozbudowy, o ile będą wykonywane zgodnie z wymogami producenta.  Urządzenia muszą być fabrycznie nowe oraz muszą pochodzić z oficjalnego kanału sprzedaży producenta na rynek Unii Europejskiej. |  |
| **I. Zakup, dostarczenie i montaż wyposażenia serwerowni tj. Pakiet 3 - Przełączniki SAN (FC) z uwzględnieniem 60 miesięcznej gwarancji w ilości 2 kpl. dla Katowickiego Centrum Onkologii –** zgodnie z SIWZ wraz z transportem sprzętu, przekazaniem do użytkowania, certyfikatami wraz z okresem gwarancji – zgodnym z szczegółowym opisem przedmiotu zamówienia  **Cena jedn. netto: …………………… zł**  **Cena netto za 2 kpl. = …………………………….zł**  **VAT %: ……… Kwota VAT:………..zł**  **Cena ogółem brutto: ………………………………………............** | | |

UWAGA:

Wszystkie parametry wymagane stanowią kryteria, których niespełnienie spowoduje odrzucenie oferty.

**Oświadczamy**, że oferowany sprzęt jest kompletny i będzie po zainstalowaniu gotowy do pracy zgodnie z jego przeznaczeniem bez konieczności dokonania dodatkowych zakupów

**.........................................................................................**

**data, podpis i pieczątka osoby uprawnionej**

**Załącznik Nr 2 do SIWZ**

**c.d. ….…….……………………..**

nazwa i adres Wykonawcy

**pieczęć firmowa**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**- OFERTA CENOWA**

**Pakiet 4**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **1. Oprogramowanie serwerowe / wirtualizacja wraz z licencjami w ilości 8 kpl.**  Nazwa oprogramowania: ………………………………………  Model/Symbol: ………………………………………  Producent: …………………………………………...  Rok produkcji: **……….** ( sprzęt fabrycznie nowy, nieużywany ) | | | | |
| **Typ** | **Minimalne parametry wymagane** | **Parametry oferowane**  **(należy podać)** |
| Oprogramowanie serwerowe –  8 sztuk (licencji) | Windows Server 2019 Standard lub równoważny, Licencje muszą umożliwić uruchomienie:  8 maszyn wirtualnych na dwóch fizycznych serwerach 2PCU/16CORE mogących pełnić rolę kontrolerów domeny na poziomie funkcjonalności lasu co najmniej 2012R, serwerów plików, serwerów DNS, DHCP, NTP, aktualizacji dla klientów sieci/stacji roboczych pracujących pod kontrolą Microsoft Windows 7,8,10 Professional, a także maszyny wirtualnej serwera kopii zapasowych i monitorowania środowiska wirtualnego, która wymaga systemu operacyjnego rodziny Microsoft Windows Server co najmniej 2008R2 SP1.  - dostęp do informacji o zakupionych licencjach takich jak:  liczba i rodzaj zakupionych licencji na określone produkty, informacje o odsprzedawcy, daty ważności numeru autoryzacyjnego, oraz klucze instalacyjne produktów przez dedykowany portal producenta   - możliwość bezpłatnego pobrania z witryny producenta produktów dostępnych w ramach zakupionej licencji  - możliwość zmiany wersji systemu operacyjnego na niższą (tzw. downgrade) |  |
| **2. Oprogramowanie dostępowe wraz z licencjami w ilości 600 kpl.**  Nazwa oprogramowania: ………………………………………  Model/Symbol: ………………………………………  Producent: …………………………………………...  Rok produkcji: **……….** ( sprzęt fabrycznie nowy, nieużywany ) | | | |
| **Typ** | **Minimalne parametry wymagane** | **Parametry oferowane**  **(należy podać)** |
| Licencje dostępowe | Licencje dostępowe CAL dla Windows Server 2019 - umożliwiające korzystanie z zasobów domeny dla 600 urządzeń/ stacji roboczych. |  |
| **3. Oprogramowanie Backup z gwarancją oraz licencjami**  Nazwa oprogramowania: ………………………………………  Model/Symbol: ………………………………………  Producent: …………………………………………...  Rok produkcji: **……….** ( sprzęt fabrycznie nowy, nieużywany ) | | | |
| **Typ** | **Minimalne parametry wymagane** | **Parametry oferowane**  **(należy podać)** |
| Całkowite koszty posiadania | * oprogramowanie musi być licencjonowanie w modelu “per-CPU”. Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. dla 4 serwerów dwuprocesorowych wyspecyfikowanych w pakiecie 1. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone * oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej * oprogramowanie musi tworzyć “samowystarczalne” archiwa, do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków * oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji * oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych w takiej puli. * oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. * oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania * oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia * oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. * oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota. * oprogramowanie musi oferować portal, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time) * oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji * oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji * oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza * oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)   oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. |  |
| Wymagania RPO | * oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej * oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych * oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora * oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn * oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server * oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej * oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) * oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 z systemem pliku ReFS jako repozytorium backupu. * oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. * oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik * oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) * oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V * oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)   oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing) |  |
| Wymagania RTO | * oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. * oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką   migrację swoimi mechanizmami   * oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków * oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta zainstalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików * oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy PowerShell Direct dla platformy Hyper-V. * oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: * Linux (ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs,) * BSD (UFS, UFS2) * Solaris (ZFS, UFS) * Mac (HFS, HFS+ ) * Windows (NTFS, FAT, FAT32, ReFS) * oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. * oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. * oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD. * oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat * oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time, przy czym funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux oraz nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia * oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych. * oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows   oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |  |
| Ograniczenie ryzyka | * oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.   oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem |  |
| Monitoring | * system musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na Microsoft Hyper-V bez   potrzeby korzystania z narzędzi firm trzecich   * system musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008R2, 2012, 2012R2 i 2016 i 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. * system musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn * system musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel * system musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk * system musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora * system musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów * system musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) * system musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna * system musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego * system musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta * system musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. |  |
| **Raportowanie** | * system raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019. * system musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. * system musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V * system musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF * system musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc * system musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach * system w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów * system musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych * system musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych * system musi mieć możliwość analizowania „przeszacowanych   wirtualnych maszyn” wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury   * system musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta * system musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. * system musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’. * system musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)   system musi mieć możliwość generowania spersonalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie |  |
| **Wsparcie techniczne:** | Oprogramowanie musi być objęte serwisem producenta przez okres 5 lat upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie Next Business Day 8x5.  Licencje muszą umożliwiać użytkowanie oprogramowania po zakończeniu okresu wsparcia serwisowego. |  |
| **I. Zakup, dostarczenie i montaż wyposażenia serwerowni tj. Pakiet 4: oprogramowanie serwerowe / wirtualizacja wraz z licencjami w ilości 8 kpl., oprogramowanie dostępowe wraz z licencjami w ilości 600 kpl., oprogramowanie Backup z gwarancją oraz licencjami dla Katowickiego Centrum Onkologii –** zgodnie z SIWZ wraz z transportem sprzętu, przekazaniem do użytkowania, certyfikatami – zgodnymi z szczegółowym opisem przedmiotu zamówienia  **Cena netto za cały Pakiet nr 4 : …………………… zł**  **VAT %: ……… Kwota VAT:………..zł**  **Cena ogółem brutto za cały Pakiet nr 4 : ……………………………………**  **w tym:** 1. Oprogramowanie serwerowe / wirtualizacja wraz z licencjami w ilości 8 kpl.  Cena jedn. netto: …………………… zł  Cena netto za 8 kpl. = …………………………….zł  VAT %: ……… Kwota VAT:………..zł  Cena ogółem brutto: ………………………………………............  2. Oprogramowanie dostępowe wraz z licencjami w ilości 600 kpl.  Cena jedn. netto: …………………… zł  Cena netto za 600 kpl. = …………………………….zł  VAT %: ……… Kwota VAT:………..zł  Cena ogółem brutto: ………………………………………............  3. Oprogramowanie Backup z gwarancją oraz licencjami  Cena jedn. netto: …………………… zł  VAT %: ……… Kwota VAT:………..zł  Cena ogółem brutto: ………………………………………............ | | | |

UWAGA: Wszystkie parametry wymagane stanowią kryteria, których niespełnienie spowoduje odrzucenie oferty.

**Oświadczamy**, że oferowany sprzęt jest kompletny i będzie po zainstalowaniu gotowy do pracy zgodnie z jego przeznaczeniem bez konieczności dokonania dodatkowych zakupów.

**........................................................................**

**data, podpis i pieczątka osoby uprawnionej**

**Załącznik Nr 2 do SIWZ**

**….…….……………………..**

**c.d.** nazwa i adres Wykonawcy

**pieczęć firmowa**

**Pakiet 5**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**- OFERTA CENOWA**

**Pakiet 5**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oprogramowanie SIEM z licencjami w ilości 1 komplet**  Nazwa: ………………………………………  Model/Symbol: ………………………………………  Producent: …………………………………………...  Rok produkcji: **……….** ( sprzęt fabrycznie nowy, nieużywany ) | | | | |
| **Lp.** | **Parametry** | **Parametry wymagane**  **bądź punktowane**  **parametry fakultatywne** | **Parametry oferowane**  **(należy podać)** |
| 1. | System do zarządzania informacją i zdarzeniami bezpieczeństwa. (SIEM Security Information and Event Management).  Jego zadaniem jest obsługa i wykrywanie zagrożeń oraz reagowanie na incydenty związane z zagrożeniem bezpieczeństwa w zakresie sieci komputerowej oraz systemów serwerowych.  System w formie maszyny wirtualnej uruchomionej w infrastrukturze Zamawiającego lub dostarczenie dedykowanego urządzenia. | TAK |  |
| 2. | Wymagania dotyczące skalowalności: |  |  |
| a. Wykonawca dokona instalacji SIEM w infrastrukturze informatycznej Zamawiającego zapewniając spełnienie łącznie wymagań w zakresie obsługi Systemu: minimum 3000 EPS, minimum 25 urządzeń jako źródeł zdarzeń, w tym minimum 8 serwerów Windows Server 2008 R2/2012/2016 z wykorzystaniem dostarczonego w ramach umowy oprogramowania typu agent; | TAK |  |
| b. System umożliwia rozszerzenie jego konfiguracji w dowolnym czasie, zapewniając spełnienie w tym samym czasie wymagań w zakresie obsługi, tj. minimum 10 000 EPS, minimum 300 urządzeń jako źródeł zdarzeń, w tym minimum 50 serwerów Windows Server 2008 R2/2012/2016/2019 z wykorzystaniem dostarczonego w ramach umowy oprogramowania typu agent; powyższe możliwe będzie do realizacji poprzez instalację dodatkowych maszyn wirtualnych przez Zamawiającego w ramach dostarczonego Systemu lub aktywacji dodatkowych licencji, co nie stanowi przedmiotu tego zamówienia i umowy. | 20 pkt. |  |
| 3. | SIEM zapewnia skalowalną architekturę spełniającą co najmniej następujące wymagania:  a. Wszystkie elementy odpowiedzialne za zbieranie informacji, dalej „Kolektory mają wydajność nie mniejszą niż 4 000 EPS każdy, przy zapewnieniu co najmniej minimalnych wymaganych parametrów środowiska uruchomieniowego;  b. Kolektory służą do przesyłania monitorowanych danych (np. zdarzeń) do warstwy je przechowującej i korelującej;  c. Kolektory buforują otrzymane informacje w wypadku awarii komunikacji pomiędzy warstwą przechowującą i korelującą a Kolektorami;  d. Komunikacja pomiędzy warstwą przechowującą i korelującą odbywa się z wykorzystaniem protokołu HTTPS, od Kolektorów do warstwy przechowującej i korelującej;  e. W wypadku awarii Kolektora, kolektor zastępczy może być uruchomiony poprzez jego zarejestrowanie w warstwie przechowującej i korelującej; konfiguracja Kolektorów nie odbywa się indywidualnie, lecz są one centralnie zarządzane; nie mogą one posiadać żadnych parametrów konfiguracyjnych poza adresami IP, które byłyby wymagane w celu uruchomienia kolektora zastępczego;  f. Kolektory przetwarzają informacje otrzymywane z wykorzystaniem protokołu NetFlow;  g. Kolektory automatycznie aktualizują nowe parsery w momencie ich zaktualizowania w centralnym systemie zarządzającym SIEM. | TAK |  |
| 4. | Warstwa przechowywania i korelacji danych, spełnia następujące wymagania: |  |  |
| a. implementacja zrealizowana w oparciu o maszynę lub maszyny wirtualne (VA – Virtual Appliance) lub dedykowane urządzenia; | TAK |  |
| b. wsparcie co najmniej następujących środowisk wirtualizacyjnych: VMWare, Hyper-V dla wdrożenia w oparciu o maszyny wirtualne; (dotyczy implementacji w formie maszyny wirtualnych) | TAK |  |
| c. SIEM nie ma ograniczeń licencyjnych związanych z ilością gromadzonych i przechowywanych zdarzeń lub danych; jedynym ograniczeniem w tym zakresie może być rozmiar przestrzeni dyskowej; | 10 PKT. |  |
| d. skalowalność SIEM wynika z możliwości dodawania kolejnych maszyn wirtualnych | 1 PKT. |  |
| możliwość wykorzystania NFS w sytuacji pracy w trybie Klastra SIEM | 1 PKT. |  |
| e. SIEM nie wymaga zastosowania dodatkowej przestrzeni dyskowej lub warstwy służącej do filtrowania lub wysyłania podzbiorów danych przesyłanych od kolektorów do warstwy korelującej; | TAK |  |
| f. zebrane dane są przechowywane w sposób skompresowany; | TAK |  |
| g.’ rozwiązanie, celem gromadzenia i przechowywania danych związanych ze zbieranymi zdarzeniami, wymagane jest wykorzystywanie nowoczesnej bazę danych noSQL; | 10 PKT |  |
| g.’’ dopuszcza się rozwiązanie, które może wykorzystywać relacyjne bazy danych np.: MS SQL, Postgresql, MySQL, Oracle, itp.; | 0 PKT |  |
| h. relacyjne bazy danych mogą być wykorzystywane do przechowywania, szablonów, zdarzeń, i innych ustrukturyzowanych informacji; | TAK |  |
| i. maszyny wirtualne SIEM działają w oparciu o system operacyjny, którego możliwość aktualizacji zapewnia Wykonawca na okres 5 lat bez ponoszenia dodatkowych kosztów przez Zamawiającego; | TAK |  |
| 5. | SIEM zbiera dane z minimum 25 monitorowanych urządzeń, również inne niż logi, co jest osiągalne poprzez:  a. aktywne wykrywanie urządzeń wewnątrz sieci bez wykorzystania dodatkowego oprogramowania typu agent oraz wsparcie dla takich protokołów jak: SNMP, WMI, SSH, JMX;  b. zdolność do monitorowania statusu oraz dostępności usług takich jak: DNS, FTP/SCP, TCP/UDP, ICMP, JDBC, LDAP, SMTP, IMAP4, POP3, POP3S, SSH, HTTP, HTTPS; wyniki powyższego monitoringu dają możliwość obliczenia poziomu dostępności danej usługi (np. procentowego).  c. możliwość wykrywania zdarzeń IPS false positive w oparciu o integrację z zewnętrznymi skanerami podatności | TAK |  |
| 6. | SIEM dostarcza zunifikowane narzędzia analityczne, dzięki którym możliwe jest wykonywanie zapytań w oparciu o ten sam język dla logów/zdarzeń zbieranych z urządzeń oraz dla danych wydajnościowych. | TAK |  |
| 7. | Kolektory SIEM pozwalają na odrzucanie danych, które uznane są za nieistotne lub niepotrzebne; mechanizm ten nie ma żadnego wpływu na model licencjonowania. | TAK |  |
| 8. | Dane w stanie surowym oraz dane sparsowane lub wzbogacone są możliwe do przesłania z Kolektorów do SIEM. | TAK |  |
| 9. | Przetwarzanie danych związanych z poszczególnymi zdarzeniami (events) wykonywane jest poprzez parsery systemowe. | TAK |  |
| 10. | Zapewnienie możliwości samodzielnej modyfikacji i poprawiania parserów. | TAK |  |
| 11. | Tworzenie własnych parserów jest w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI). | TAK |  |
| 12. | Tworzenie nowych atrybutów (sparsowanych zmiennych), urządzeń oraz rodzajów zdarzeń (events) jest w całości możliwe z wykorzystaniem interfejsu graficznego (GUI) bez użycia linii komend (CLI). | TAK |  |
| 13. | Parsery są tworzone z wykorzystaniem narzędzi wspierających dla XML (XML framework). | TAK |  |
| 14. | Zapewnienie możliwości monitorowania urządzeń bez wykorzystania aplikacji typu agent oraz poprzez SSH, telnet, WMI, JMX. | TAK |  |
| 15. | SIEM umożliwia zbierania zdarzeń (event) z systemów Windows w oparciu o aplikacje typu agent. | TAK |  |
| 16. | SIEM wspiera obsługę aplikacji typu agent na systemy Windows, tj. Windows Agent, które posiadają co najmniej następujące możliwości: |  |  |
| a. centralne zarządzanie; | TAK |  |
| b. zbieranie logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows; | TAK |  |
| c. zbieranie logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application; | TAK |  |
| d. monitorowanie rejestru, urządzeń zewnętrznych (removable devices) oraz integralności plików; | 2 PKT. |  |
| e. wykonywanie poleceń PowerShell wraz z odesłaniem wyniku ich działania w postaci logów; | 2 PKT. |  |
| f. wykonywanie poleceń WMI wraz z odesłaniem wyniku ich działania w postaci logów; | 2 PKT. |  |
| g. agent instalowany na systemach z rodziny Windows komunikuje się z poszczególnymi komponentami SIEM w sposób zaszyfrowany z wykorzystaniem protokołu SSL. | TAK |  |
| 17. | Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Linux (Linux Agent), które posiadają nie mniej niż następujące możliwości:  a. centralne zarządzanie  b. możliwość zbierania logów z wykorzystaniem protokołu syslog  c. możliwość zbierania logów z plików tekstowych  d. zdolność do monitorowania integralności plików  e. zdolność do monitorowania pliku w oparciu o jego proces rodzimy oraz sumę kontrolną | TAK |  |
| 18. | SIEM zapewnia wsparcie dla zarządzania w oparciu o role (Role Based Administration) celem ograniczania dostępu do danych oraz do GUI. | TAK |  |
| 19. | a. SIEM wykrywa usługi Active Directory i LDAP oraz wyświetla informacje o strukturze katalogowej drzewa w GUI. | 5 PKT. |  |
| 20. | b. SIEM umożliwia wykorzystanie struktury katalogowej drzewa jako warunku podczas tworzenia raportów i w ramach pozostałych mechanizmów analitycznych. | 5 PKT. |  |
| 21. | SIEM zapewnia wspieranie zewnętrznych metod uwierzytelniania, co najmniej w zakresie: Active Directory, LDAP. | TAK |  |
| SIEM zapewnia możliwość integracji z zewnętrznymi bazami danych o zagrożeniach (Threat Intelligence feeds - TI): | TAK |  |
| a. wsparcie dla plików CSV musi być wykonywalne z wykorzystaniem interfejsu graficznego GUI; | TAK |  |
| b. definicje w ramach integracji muszą zawierać co najmniej: adresy IP, domeny, sumy kontrolne (hash), adresy URL; | TAK |  |
| c. wymagane jest aby każda z zewnętrznych baz zagrożeń była w stanie wesprzeć do 200 tys. wpisów; | TAK |  |
| d. zestaw komercyjnych baz zagrożeń oraz zestaw baz zagrożeń niekomercyjnych (open source), obydwa zestawy zintegrowane z SIEM i dostarczone wraz z Systemem; | TAK |  |
| e. SIEM umożliwia korelację informacji z baz zagrożeń z danymi otrzymywanymi w czasie rzeczywistym; korelacja ta odbywa się w pamięci systemu względem otrzymywanych danych o zdarzeniach (event data); | TAK |  |
| f. wykorzystanie funkcjonalności Geo IP w oparciu o bazę pochodzącą od tego samego producenta | TAK |  |
| g. SIEM umożliwia korelację informacji z baz zagrożeń z danymi historycznymi. | 5 PKT. |  |
| 22. | SIEM dostarcza następujące rodzaje raportów: PCI-DSS, HIPAA, FISMA, ISO, GLBA, GPG13, SANS Critical Controls. | 2 PKT. |  |
| 23. | SIEM umożliwia eksportowanie i importowanie pulpitów administracyjnych (dashboards), raportów oraz reguł w formacie XML. | 1 PKT. |  |
| 24. | SIEM umożliwia zbieranie konfiguracji urządzeń, identyfikowanie zmian w nich następujących wraz z możliwością porównywania poszczególnych wersji.  a. wykryte urządzenie ma posiadać swoją reprezentację w bazie urządzeń w ramach dostarczonego rozwiązania SIEM co jednocześnie ma umożliwiać prezentację następujących informacji (nie mniej niż):  i. wersja oprogramowania/firmware/systemu operacyjnego  ii. numer seryjny urządzenia  iii. skonfigurowane interfejsy wraz z:  1. nazwą interfejsu  2. adresem IP oraz podsiecią  3. statusem interfejsu (włączony, wyłączony)  4. informacją o skonfigurowanych poziomach bezpieczeństwa  5. prędkością interfejsu  6. możliwością edycji nazwy oraz prędkości interfejsu  iv. procesach działających na urządzeniu lub systemie operacyjnym  v. alarmach w przypadku zmiany statusu procesu np. jego uruchomienia lub zatrzymania  b. możliwość automatycznego przypisania do grupy poszczególnych urządzeń znajdujących się w bazie urządzeń, np. grupa serwerów Windows, grupa rozwiązań firewall, etc.  c. automatyczne wykrywanie aplikacji działających na poszczególnych urządzeniach. Wymagane jest aby baza urządzeń miała możliwość konfiguracji grup aplikacji celem automatycznego umieszczania w nich poszczególnych urządzeń, np. grupa aplikacyjna "IIS Servers" wyświetla wszystkie urządzenia z uruchomionymi usługami Microsoft IIS  d. raportowanie informacji zawartych w bazie urządzeń, w tym takich jak:  i. raportowanie na temat firmware'u poszczególnych urządzeń lub numeru jego wersji  ii. raport audytowy z informacją typu "pass/fail" analizujący czy określone urządzenia działają z właściwą wersją firmware'u/systemu operacyjnego  e. wymagane jest aby rozwiązanie SIEM posiadało wbudowany szablon, który po przeprowadzeniu aktywnego wykrywania urządzeń będzie pozwalał na automatyczne określenie jakiego rodzaju dane będą z nich zbierane oraz jaki będzie interwał ich pobierania.  f. zbieranie metryk wydajnościowych ma dotyczyć nie mniej niż:  i. utylizacji interfejsów sieciowych, występujących tam błędów, ilości wysłanych i odebranych danych (np. bajtów)  ii. obciążenia CPU  iii. wykorzystania pamięci  iv. wykorzystania przestrzeni dyskowej  v. utylizacji poszczególnych procesów | 10 PKT. |  |
| 25. | Pulpity administracyjne (dashboards) umożliwiają wspólną prezentację. | TAK |  |
| 26. | Dane w ramach pulpitów administracyjnych pozwalają na następujące formy prezentacji: Bar, Pie, Line, Table, Combination (line and table view), Treemap, Scatter graph, Single values, Gauges, Geographical Map. Wartości graniczne (thresholds) w kolorach czerwonym, bursztynowym oraz zielonym mogą być definiowane w razie potrzeby na poszczególnych wykresach. | 1 PKT. |  |
| 27. | W ramach notyfikacji oraz zarządzania incydentami SIEM zapewnia:  a. narzędzia pozwalające na samodzielne tworzenie polityk informujących o incydentach;  b. możliwość uruchamiania skryptów w odpowiedzi na wybrane incydenty;  c. możliwość integracji w oparciu o API z zewnętrznymi systemami do obsługi zgłoszeń (ticketing systems)  d. wbudowany mechanizm obsługi zgłoszeń (ticketing system). | TAK |  |
| 28. | W ramach analityki SIEM zapewnia: |  |  |
| a. wyszukiwanie zdarzeń (events) w czasie rzeczywistym; | TAK |  |
| b. wyszukiwanie w oparciu o słowa kluczowe oraz w oparciu o sparsowane atrybuty zdarzeń względem analizowanych danych; | TAK |  |
| c. wyszukiwanie historyczne z zastosowaniem kwerend typu SQL, ze wsparciem filtrowania typu Boolean, grupowanie w oparciu o agregację danych, filtry czasowe, wyrażenia regularne, wyrażenia matematyczne. Opisane możliwości muszą być dostępne zarówno przez GUI, jak i API. | TAK |  |
| d. wyszukiwanie w oparciu o co najmniej następujące operatory: include =,!=, <,>, IS NULL, IS NOT NULL, contains, not contains, contains regex, not contains regex; | 1 PKT. |  |
| e. podejmowanie w czasie rzeczywistym działań w oparciu o złożone wzorce zdarzeń:  ⁻ w przypadku prostych zapytań możliwość np. określenia wartości granicznej (threshold) ilości zdarzeń X w określonym przedziale czasowym Y z wybranych wartości, | TAK |  |
| ⁻ w przypadku zapytań przekrojowych wspierających filtry typu Boolean: |  |  |
| ○ możliwość stworzenia wzorców zapytań za określony przedział czasu z wykorzystaniem operatorów takich jak: AND, OR, FOLLOWED BY, AND NOT, and NOT FOLLOWED\_BY,  ○każdy z wzorców umożliwiający filtrowanie i agregowanie z wykorzystaniem operatorów takich jak: AVG, MAX, MIN, COUNT and COUNT DISTINCT, | 2 PKT. |  |
| ○ ustalane wartości graniczne (thresholds) mogą być statyczne lub też mogą być otrzymywane jako rezultat analizy statystycznej; analiza statystyczna i alarmowanie w oparciu o zdarzenia działa w oparciu o średnie kroczące (moving averages) i odchylenia standardowe (standard deviations), a w wypadku przekroczenia statystycznej wartości granicznej (statistical threshold) zostaje wygenerowany alert w czasie zbliżonym do rzeczywistego; | 1 PKT. |  |
| f. wykorzystywania obiektów wykrytych i znajdujących się bazie urządzeń, użytkowników i ich tożsamości oraz lokalizacji podczas wyszukiwania i tworzenie reguł | TAK |  |
| g. tworzenie harmonogramu raportów i dostarczanie ich pocztą elektroniczną wraz z możliwością eksportowania do formatów CSV i PDF; | TAK |  |
| h. wyszukiwanie zdarzeń poprzez pryzmat całej organizacji lub też w ujęciu fizycznego lub logicznego obszaru raportującego; | TAK |  |
| i. wykorzystanie dynamicznych list pozwalających na obserwację źródeł generujących zdarzenia krytyczne, wraz z możliwością wykorzystania tych list w dowolnej regule raportującej; | TAK |  |
| j. skalowanie możliwości analitycznych poprzez dodawanie do SIEM kolejnych maszyn wirtualnych bez konieczności wyłączania całego SIEM lub wymiany dostarczonego urządzenia; | 1 PKT. |  |
| k. automatyczne korelowanie użytkownika z jego lokalizacją i adresem IP;  ⁻ tworzenie raportów i wyszukiwanie użytkownika w połączeniu z jego adresem IP oraz lokalizacją; lokalizacja może oznaczać port na switch’u, adres MAC lub połączenie VPN;  ⁻ wzbogacanie zdarzeń (events) przy których dane użytkownika pozbawione są informacji o adresie IP. | TAK |  |
| l. System musi mieć możliwość anonimizacji zebranych danych w zakresie nie mniejszym niż: adresy IP, nazwy hostów, adres MAC, adresy email, nazwy użytkowników. Proces ten ma być możliwy w oparciu o role/profile użytkowników administracyjnych. Ujawnienie danych (deanonimizacja) ma sie odbywać z wykorzystaniem użytkownika udzielającego lub zabraniającego jej wykonania. W przypadku zatwierdzenia wspomnianego żądania, dane są ujawniane na określony czas, po którym powtórnie ulegają anonimizacji. | 10 PKT. |  |
| 29. | SIEM pozwala na realizowane w oparciu o polityki archiwizowanie danych do innego udziału, takiego jak np. NFS, przy zapewnieniu możliwości odtwarzania tych danych z wykorzystaniem GUI. | TAK |  |
| 30. | Integralność danych związanych ze zdarzeniami jest weryfikowalna z wykorzystaniem GUI w oparciu o przeliczenie sum kontrolnych, które obliczane były w momencie zapisywania danych o zdarzeniach na dysk SIEM. | TAK |  |
| 31. | W celu instalacji SIEM jako maszyny wirtualnej Zamawiający udostępni niżej wymienione zasoby na platformie Hyper-V:  ● do 8 wirtualnych rdzeni 2,1 GHz  ● do 32 GB RAM  ● do 1 TB przestrzeni dla danych  W przypadku wymagań systemu większych niż podane, wymagane jest dostarczenie dedykowanego urządzenia lub serwera przy zachowaniu wymagań skalowalności określonych w punkcie 2b. | TAK |  |
| 32. | Wykonawca dokona instalacji polegającej na podstawowej konfiguracji i uruchomieniu SIEM w infrastrukturze informatycznej Zamawiającego w terminie 30 dni od dnia zawarcia umowy. | TAK |  |
| 33. | W ramach instalacji Wykonawca przeprowadzi instruktaż obejmujący instalację i administrowanie Systemem dla 3-5 pracowników Zamawiającego, trwający nie krócej niż 8 godzin. | TAK |  |
| 34. | Wykonawca zobowiązany jest w okresie 6 miesięcy od dnia podpisania protokołu odbioru zainstalowanego i uruchomionego Systemu, zapewnić Zamawiającemu efektywne wsparcie umożliwiające prawidłowe działanie Systemu i pomoc, w formie konsultacji, w obsłudze Systemu, polegające w szczególności na dostosowywaniu System do potrzeb Zamawiającego (dokonaniu optymalizacji konfiguracji Systemu zgodnie z wymaganiami Zamawiającego) oraz zapewnić optymalizację konfiguracji Systemu wynikające z praktyki jego stosowania przynajmniej w zakresie ilości urządzeń określonych w punktach 2a,5a oraz usług i protokołów określonych w punkcie 5b. Wykonawca na każde żądania Zamawiającego udzieli wsparcia w zakresie obsługi Systemu oraz bezzwłocznie przywróci jego funkcjonalności w przypadku wystąpienia nieprawidłowości w działaniu. | TAK |  |
| 35. | W terminie 1 miesiąca od dnia podpisania protokołu odbioru Systemu Wykonawca przedstawi Zamawiającemu do akceptacji dokumentację techniczną Systemu, obejmującą co najmniej:  a) plan i opis architektury logicznej SIEM;  b) opis funkcji SIEM do zaimplementowania w infrastrukturze Zamawiającego; szczegółowy zakres integracji SIEM z innymi systemami eksploatowanymi w infrastrukturze Zamawiającego;  c) opis zakresu prac niezbędnych do dostosowania Systemu do potrzeb Zamawiającego i optymalizacji konfiguracji środowiska produkcyjnego, sekwencji (harmonogramu) tych prac, wskazanie osób odpowiedzialnych za ich realizację w imieniu Zamawiającego i Wykonawcy. | TAK |  |
| 36. | Wykonawca zagwarantuje w łącznym czasie co najmniej 60 godzin realizację usług optymalizacji konfiguracji Systemu oraz optymalizacji środowiska w jakim pracuje System opisanych w pkt 34 i 35. Zadania realizowane będą każdorazowo po uzgodnieniu z Zamawiającym lub na jego żądanie. Po zakończeniu zadania Wykonawca dokona aktualizacji dokumentacji technicznej Systemu. | TAK |  |
| 37. | Wykonawca gwarantuje następujące czasy naprawy Systemu i przywrócenia jego wymaganej funkcjonalności, licząc od chwili zgłoszenia przez Zamawiającego:  ● 24 godziny w przypadku Awarii SIEM, co rozumie się jako niedostępność Systemu lub awarię Systemu, która uniemożliwia jego wykorzystanie;  ● 120 godzin w przypadku Błędu w SIEM, co rozumie się jako nieprawidłowe działanie Systemu lub jego komponentów, które uniemożliwia lub ogranicza prawidłowe działanie SIEM. | TAK |  |
| 38. | Wykonawca udziela gwarancji na wykonane usługi w zakresie wsparcia Systemu, na okres 12 miesięcy od dnia podpisania bez zastrzeżeń protokołu odbioru tych usług, wraz z przyjęciem bez zastrzeżeń „Dokumentacji powykonawczej”, o czym mowa w punkcie 39.  W okresie gwarancji Wykonawca zobowiązany jest do usuwania wszelkich nieprawidłowości i błędów związanych z konfiguracją Systemu oraz aktualizacji Dokumentacji powykonawczej, a także do wprowadzania wszelkich zmian w Dokumentacji powykonawczej, zapewniających poprawność konfiguracji Systemu w odniesieniu do zdiagnozowanych nieprawidłowości i błędów będących faktycznym błędem wykonawcy, w terminie nie dłuższym niż 14 dni od dnia ich zgłoszenia przez Zamawiającego. Wykonawca niezwłocznie dostarczy Zamawiającemu poprawioną Dokumentację w formie elektronicznej.  Niezależnie od udzielonej gwarancji Zamawiającemu przysługuje rękojmia na wykonane usługi w zakresie wsparcia Systemu. | TAK |  |
| 39. | DOKUMENTACJA POWYKONAWCZA  W terminie 7 dni od zakończenia usług w zakresie wsparcia Systemu Wykonawca sporządzi i dostarczy Zamawiającemu, w formie elektronicznej i papierowej opracowanie pn. „Dokumentacja powykonawcza”, które obejmuje następujące elementy:  ● Ogólny opis Systemu (SIEM)  ● Wykaz całościowy oprogramowania oraz licencji wykorzystywanych w ramach wdrożonego SIEM, w tym systemy operacyjne, bazy danych, serwery aplikacyjne, itp.  ● Architektura logiczna Systemu; graficzna prezentacja Systemu i jego połączeń wraz z opisem  ● Przepływ danych w Systemie, tj. koncepcja obiegu informacji w Systemie pomiędzy poszczególnymi komponentami, warstwami Systemu  ● Polityka aktualizacji Systemu i testowania jego zmian  ● Specyfikacja i konfiguracja serwerów wirtualnych  ● Szczegółowa konfiguracja poszczególnych elementów Systemu, tj. serwery zarządzające, serwery baz danych, systemy operacyjne, serwery aplikacyjne, serwery www - zrzuty ekranów, pliki konfiguracyjne, opisy konfiguracji, opisy uruchomionych usług, opisy poszczególnych funkcji Systemu  ● Systemy zależne, np. agenty na innych serwerach, dodatkowe oprogramowanie na innych stacjach roboczych i serwerach współpracujące z Systemem, opis integracji z innymi usługami w tym w szczególności z MS Active Directory oraz MS Exchange  ● Architektura sieciowa Systemu, tj. opis połączeń sieciowych pomiędzy poszczególnymi elementami, adresacja IP, umiejscowienie elementów Systemu w poszczególnych strefach: DMZ, LAN, Internet  ● Opis portów komunikacyjnych, zawierający informacje o otwartych portach oraz sposób zabezpieczenia zbędnych/nieużywanych portów  ● Rodzaje kont systemowych i ich uprawnienia, tj. określenie standardowych profili uprawnień, sposobu zarządzania użytkownikami oraz uprawnieniami w Systemie  ● Zarządzanie hasłami, tj. opis sposobu przechowywania haseł w Systemie,  ● Uprawnienia kont serwisowych  ● Role administracyjne  ● Ustawienia polityki haseł  ● Procedury zmiany haseł serwisowych, administracyjnych i użytkownika  ● Procedury weryfikacji uprawnień  ● Konfiguracja reguł firewall  ● Bezpieczeństwo transmisji, tj. opis rozwiązań w zakresie zapewnienia poufności transmisji danych w sieci LAN/DMZ oraz Internet  ● Ochrona konfiguracji Systemu, tj. ochrona krytycznych plików konfiguracyjnych  ● Opis rozwiązań w zakresie logowania zdarzeń, tj. wskazanie rodzajów oraz lokalizacji dzienników w Systemie, opis logowanych zdarzeń, w przypadku niestandardowych logów opis ich struktury  ● Ochrona dzienników, tj. opis sposobu zabezpieczenia zapisów w logach przed ich utratą oraz nieuprawnioną zmianą, informacja o czasie przechowywania logów, możliwości przekazania logów do systemów zewnętrznych  ● Procedura odtwarzania Systemu, tj. opisanie procedury backupu i odtworzenia całego Systemu i jego poszczególnych elementów, określenie czasu potrzebnego na odtworzenie całego Systemu oraz jego poszczególnych elementów, opis procedur przywracania Systemu do pełnej funkcjonalności po awarii  ● Procedura instalacji Systemu, tj. opis procedury instalacji Systemu „od początku - krok po kroku”, opis wszystkich kroków instalacji i konfiguracji Systemu w postaci zrzutów ekranu z opisami  ● Procedury wykonywania krytycznych operacji w Systemie, tj. migracja, aktualizacja, itp.  ● Instrukcje obsługi Systemu dla Administratorów.  ● Wykaz prac/działań przeprowadzonych w ramach usługi wsparcia Systemu | TAK |  |
| 40. | Użyteczność oraz dojrzałość technologiczna zaoferowanego rozwiązania musi być potwierdzona obecnością producenta rozwiązania w Magicznym Kwadrancie Gartnera (MQ) dla Security Information and Event Management (SIEM) z 2020 roku. | 30 PKT. |  |
| 41. | System objęty jest licencją na czas nieokreślony, a także podstawowym wsparciem technicznym producenta Systemu lub jego autoryzowanego partnera na okres 5 lat od dnia uruchomienia licencji Systemu. Podstawowe wsparcie techniczne producenta obejmuje pomoc przy instalacji Systemu oraz przy jego późniejszej eksploatacji.  W ramach podstawowego wsparcia technicznego Zamawiający otrzymuje:  ● bezpłatny dostęp do aktualizacji, poprawek i nowych wersji/kompilacji programu,  ● wsparcie online 8x5,  ● wsparcie telefoniczne w godzinach pracy supportu producenta,  ● dostęp do bazy wiedzy oraz dokumentacji SIEM,  ● dostęp do forum dotyczącego SIEM, o ile takie forum istnieje. | TAK |  |
| **I. Zakup, dostarczenie i montaż wyposażenia serwerowni tj. Pakiet 5 – oprogramowanie SIEM wraz z licencjami dla Katowickiego Centrum Onkologii –** zgodnie z SIWZ wraz z transportem, przekazaniem do użytkowania, konfiguracją i uruchomieniem, certyfikatami wraz z okresem gwarancji – zgodnym z szczegółowym opisem przedmiotu zamówienia  **Cena jedn. netto: …………………… zł**  **Cena netto za kpl. = …………………………….zł**  **VAT %: ……… Kwota VAT:………..zł**  **Cena ogółem brutto: ………………………………………............** | | | |

**UWAGA:**

Wszystkie parametry wymagane stanowią kryteria, których niespełnienie spowoduje odrzucenie oferty.

**Oświadczamy**, że oferowany sprzęt jest kompletny i będzie po zainstalowaniu gotowy do pracy zgodnie z jego przeznaczeniem bez konieczności dokonania dodatkowych zakupów

**.........................................................................................**

**data, podpis i pieczątka osoby uprawnionejZałącznik Nr 4 do SIWZ**

**….…….……………………..**

nazwa i adres Wykonawcy

**pieczęć firmowa**

## ISTOTNE POSTANOWIENIA UMOWY

UMOWA NR ………………..

zawarta w dniu ..................... w Katowicach

pomiędzy:

### Katowickim Centrum Onkologii

z siedzibą w 40 – 074 Katowice, ul. Raciborska 26

wpisanym do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji i publicznych zakładów opieki zdrowotnej Krajowego Rejestru Sądowego pod numerem **KRS 0000096116**

posiadającym NIP 634-22-99-376, Regon 276201240

reprezentowanym przez

lek. med. Włodzimierza Migacza – Dyrektora

zwanym dalej **Zamawiającym**

a

**\*………………………………………………………………………**

z siedzibą w \*……………………………….

wpisaną do \*……………………………………………

posiadającą NIP \*………………………… Regon **\***…………………………………

reprezentowaną przez:

\*……………………………………………………………………..

zwaną dalej **Wykonawcą**

**§1**

Wykonawca wyłoniony w wyniku udzielenia zamówienia publicznego w trybie przetargu nieograniczonego na zakup, dostarczenie i montaż wyposażenia serwerowni **Pakiet nr …** dla Katowickiego Centrum Onkologii, zgodnie z **Załącznikiem Nr 1 do Umowy** sporządzonym na podstawie Załącznika nr 2 do SIWZ - Szczegółowy opis przedmiotu zamówienia – Oferta Cenowa przyjmuje do wykonania niżej wymieniony zakres, zgodnie ze SIWZ, złożoną ofertą z dnia **……. r.**

**§2**

1. Wykonawca zobowiązuje się do wykonania zamówienia w terminie do ……… tygodni od wezwania, nie później niż do 30 czerwca 2021.

2. Wykonawca zapewnia dostarczenie i montaż wyposażenia serwerowni dla Katowickiego Centrum Onkologii wraz z licencjami bezterminowymi.

3. Potwierdzeniem wykonania przedmiotu umowy będzie „Protokół odbioru przedmiotu zamówienia” podpisany przez przedstawicieli Zamawiającego i Wykonawcy.

4. Osoby uprawnione do podpisania „ Protokołu odbioru przedmiotu zamówienia”

ze strony Zamawiającego:

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

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

ze strony Wykonawcy:

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

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

**§3**

1.Za realizację przedmiotu umowy określonego w §1 strony ustalają wynagrodzenie za:

**Pakiet …..**, **zgodnie z Załącznikiem nr 1 do Umowy**

**netto za kpl. = …………………………….zł**

**podatek VAT %: ……… Kwota VAT:………..zł**

**brutto: ………………………………………............**

**brutto (słownie): ………………………………………............**

2. Dopuszcza się wprowadzenie odpowiednich zmian wysokości wynagrodzenia Wykonawcy, w przypadku zmiany (Dotyczy Pakietu nr 1 i Pakietu nr 2):

1) stawki podatku od towarów i usług,

2) wysokości minimalnego wynagrodzenia za pracę ustalonego na podstawie [art. 2 ust. 3-5](https://sip.legalis.pl/document-view.seam?documentId=mfrxilruguytcobxge3c44dboaxdcmbvg44tmmjv) ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę,

3) zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne.

4) Zasada i tryb wprowadzenia zmiany w przypadku określonym w ust. 4 pkt 1) to podpisany przez Strony aneks obowiązujący od daty rozpoczęcia obowiązywania aktu prawnego wprowadzającego zmianę, zaś w przypadku opisanym w ust. 4 pkt 2) i pkt 3) zmiana wprowadzana będzie na wniosek Strony w terminie 30 dni w formie aneksu do umowy po udokumentowaniu, że zmiany, o których mowa w ust. 4 pkt 2) lub pkt 3) będą miały wpływ na koszty wykonania zamówienia przez wykonawcę o ten koszt, po wykazaniu przez Wykonawcę przy pomocy dokumentów wpływu zmiany wskazanych regulacji na koszty wykonania zamówienia i będzie wykazywała realny wpływ zmiany obciążeń publicznoprawnych na koszty wykonania zamówienia, a Wykonawca przy pomocy dokumentów i obliczeń wykaże koszty zmian, które w formie dokumentów zostaną załączone do umowy, w szczególności będą to kalkulacje kosztów pracy z oferty, w stosunku do kosztów pracy wynikających ze zmiany przepisów.

3. Zwaloryzowana cena stanowić będzie za każdym razem kolejny Aneks do Umowy (Dotyczy Pakietu nr 1 i Pakietu nr 2):.

**§4**

1. Wynagrodzenie płatne będzie w 24 równych miesięcznych ratach w wysokości każdej raty …………… zł brutto, w tym cena sprzętu ………….zł brutto, koszt finansowania ……..zł brutto

- dotyczy Pakiet nr 1 i 2 .

2. Zamawiający ma możliwość wcześniejszej zapłaty za sprzęt w takim wypadku zapłacie podlega jedynie cena sprzętu bez kosztów finansowania za niewykorzystany okres - dotyczy Pakiet nr 1 i 2 .

3. a) Wynagrodzenie płatne w terminie 30 dni od daty otrzymania przez Zamawiającego faktury VAT, przy czym faktura VAT musi zawierać cenę zakupu oraz wartość finansowania z tytułu sprzedaży ratalnej. Pierwszą fakturę Wykonawca wystawi po podpisaniu przez strony „Protokołu odbioru przedmiotu zamówienia” - dotyczy Pakiet nr 1 i 2.

b) Wynagrodzenie płatne w terminie 30 dni od daty otrzymania przez Zamawiającego faktury VAT - dotyczy Pakiet nr 3, 4 i 5 .

4. Na żądanie Zamawiającego w sprawie całościowej spłaty pozostałej części należności głównej wyrażone na co najmniej 7 dni przed terminem złożenia kolejnej faktury Wykonawca będzie zobowiązany do wystawienia faktury VAT za pozostałą wartość sprzętu - dotyczy Pakiet nr 1 i 2.

5. Strony akceptują wystawianie faktur Vat w formie elektronicznej, zgodnie z art. 106n ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (tj. Dz.U. z 2020 r., poz. 106, z późn. zm.). Faktury elektroniczne będą Zamawiającemu wysyłane na adres e-mail: …………… Zamawiający zobowiązuje się do poinformowania Wykonawcy o każdorazowej zmianie ww. adresu mailowego. Osobą upoważnioną do kontaktów w sprawie e-faktur ze strony Zamawiającego jest ……………………. Jednocześnie Zamawiający informuje, że istnieje możliwość korzystania przez Wykonawców z platformy elektronicznego fakturowania, pod adresem: <https://brokerpefexpert.efaktura.gov.pl>.

6.Faktury muszą spełniać wymogi obowiązujących przepisów co do formatu faktury, np. XML.

7. Płatność uregulowana zostanie na rachunek Wykonawcy Nr**……………………………**

**§5**

1. Na dostarczony sprzęt serwerowy/oprogramowanie zgodne z wymaganiami opisanymi w **SIWZ** Wykonawca 60 miesięcznej gwarancji standardowej producenta ( okres gwarancji jest równy okresowi rękojmi) licząc od daty podpisania przez Strony Umowy „Protokół odbioru przedmiotu zamówienia” i zapewnia sprawność w okresie jej obowiązywania, przy czym warunki gwarancji obejmują w szczególności:

1. usługi w ramach gwarancji będą realizowane w siedzibie Zamawiającego,
2. czas reakcji serwisu - do końca następnego dnia roboczego od chwili zgłoszenia,
3. możliwość zgłaszania awarii w trybie 24-godzinnym przez 7 dni w tygodniu,
4. serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta,
5. w przypadku awarii dysku twardego – uszkodzony dysk pozostaje u Zamawiającego,
6. gwarancja nie będzie ograniczać rekonfiguracji lub rozbudowy, o ile będą wykonywane zgodnie z wymogami producenta.
7. Wykonawca wniesie zabezpieczenie należytego wykonania umowy w wysokości ............................. złotych, (słownie: .......................................................................... złotych) w formie ........................., najpóźniej w dniu zawarcia Umowy.
8. Zabezpieczenie służy do pokrycia roszczeń Zamawiającego z tytułu niewykonania lub nienależytego wykonania Umowy.
9. Zamawiający zwróci zabezpieczenie:

a) w terminie 30 dni po podpisaniu „Protokołu odbioru przedmiotu zamówienia” przez  upoważnionego przedstawiciela ze strony Zamawiającego i Wykonawcy w wysokości-**70%,**

b) w terminie 15 dni po wygaśnięciu rękojmi w wysokości -  **30%** (przy czym okres rękojmi nie może być krótszy niż okres gwarancji łącznej).

**§6**

1. Wykonawca zobowiązuję się zapłacić Zamawiającemu następujące kary umowne:

1. za opóźnienie w realizacji dostawy ponad termin, o którym mowa w **§ 2** ust.1, w wysokości **0,1%** wartości umowy za każdy rozpoczęty kolejny dzień kalendarzowy opóźnienia,
2. za brak naprawy sprzętu/oprogramowania do 3 dni roboczych w wysokości **0,2%** wartości umowy za każdy rozpoczęty kolejny dzień roboczy,
3. za brak sprawności sprzętu/oprogramowania powyżej 15 dni roboczych w okresach 12-miesięcznych, w wysokości **0,2 %** wartości umowy za każdy rozpoczęty kolejny dzień,
4. za brak sprawności sprzętu/oprogramowania ( rozumianej jako brak zachowania całkowitej funkcjonalności) powyżej 25 dni roboczych w okresach 12-miesięcznych, w wysokości **2%** wartości umowy za każdy rozpoczęty kolejny dzień.

2. Kwoty z tytułu kary umownej są płatne w terminie 7 dni od dnia wezwania Wykonawcy do ich zapłaty. W przypadku, w którym płatność kwot kary umownej nie zostanie dokonana w powyższym terminie, Wykonawca wyraża zgodę na potrącenie kwot naliczonej kary umownej z przysługującego mu wynagrodzenia, poprzez zmniejszenie zapłaty z wystawionych przez Wykonawcę faktur VAT.

**§7**

1. Wykonawca gwarantuje prawidłowe i rzetelne wykonanie niniejszej Umowy.

2. Wykonawca zobowiązuje się wykonać przedmiot zamówienia:

* 1. zgodnie z obowiązującymi przepisami,
  2. zgodnie z wymaganiami producenta urządzenia.

**§8**

1. Za nienależyte wykonanie umowy uznaje się niezachowanie pełnej funkcjonalności sprzętu/oprogramowania w okresie ponad 30 dni w roku kalendarzowym.

2. Za niewykonanie Umowy uznaje się niepodpisanie Protokołu odbioru przedmiotu zamówienia w terminie do 30 czerwca 2021r.

3. Odmowę płatności z tytułu kar umownych uznaje się za nienależyte wykonanie umowy.

4. W przypadku niewykonania lub nienależytego wykonania umowy przez Wykonawcę zapłaci on karę  umowną w wysokości wniesionego zabezpieczenia należytego wykonania umowy,   
a Zamawiający będzie mógł rozwiązać umowę na podstawie jednostronnego oświadczenia bez okresu wypowiedzenia.

5. Wykonawca ponosi odpowiedzialność za szkody w związku z wykonaniem Umowy, przy czym Zamawiający zastrzega sobie również możliwość dochodzenia odszkodowania na drodze cywilnoprawnej w zakresie zarówno rzeczywistej straty, jak i utraconych korzyści.

§**9**

1. Wykonawca nie będzie zbywać wierzytelności wynikających z realizacji niniejszej Umowy bez uprzedniej pisemnej zgody Zamawiającego z uwzględnieniem wymogów określonych w ustawie o działalności leczniczej.

2. Wykonawca nie będzie dokonywał czynności prawnych ze zobowiązaniami wynikającymi z zawartej umowy, w tym wyłącza się możliwość: poręczenia za zobowiązania szpitala przez podmiot trzeci (wstąpienie w prawa zaspokojonego wierzyciela), tj. Wykonawca zobowiązuje do nie zawierania umowy poręczenia przez osoby trzecie za długi Zamawiającego należne na podstawie niniejszej umowy (w rozumieniu art. 876-887 Kc) – w razie niewywiązania się z niniejszego zobowiązania Wykonawca zapłaci Zamawiającemu karę umowną w wysokości wartości świadczenia, które poręczyciel spełni wobec Wykonawcy, jak również Wykonawca zobowiązuje się do niedokonywania przekazu świadczenia Zamawiającego (w rozumieniu art. 9211- 9215 Kc) w całości lub w części należnego na podstawie niniejszej umowy, w razie niewywiązywania się z niniejszego zobowiązania Wykonawca zapłaci Zamawiającemu karę umowną w wysokości wartości przekazanego świadczenia.

§**10**

1.**Umowa obowiązuje od dnia ………………r. do dnia …………….r.**

2. Zamawiający zastrzega sobie, że będzie uprawniony do odstąpienia od umowy w trybie art. 145 ustawy z dnia  29 stycznia 2004r.– Prawo zamówień publicznych (t.j.: Dz. U. z 2019r., poz. 1843 z późn. zm.) w razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili jej zawarcia, w terminie 30 dni od powzięcia wiadomości o tych okolicznościach.

3. Zamawiający zastrzega sobie możliwość wypowiedzenia umowy z zachowaniem 30 dniowego okresu wypowiedzenia.

**§11**

1. Spory powstałe na tle niniejszej umowy rozstrzygać będzie Sąd właściwy dla siedziby Zamawiającego.

2. Zmiany niniejszej umowy mogą nastąpić wyłącznie w formie pisemnej na podstawie podpisanego przez  Strony Aneksu do Umowy.

**§12**

W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (t.j.: Dz. U. z 2019r., poz. 1843 z późn. zm.) i Kodeksu cywilnego.

**§13**

Niniejszą umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

**WYKONAWCA ZAMAWIAJĄCY**

**UWAGA !**

- prosimy o wypełnienie pól oznaczonych gwiazdką

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

**data, podpis i pieczątka osoby uprawnionej**

##### Załącznik Nr 5 do SIWZ

**................................................**

**Nazwa i adres Wykonawcy**

**Pieczątka firmowa**

**OŚWIADCZENIE WYKONAWCY W SPRAWIE**

**GWARANCJI ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY**

**Oświadczam**, że w przypadku wniesienia zabezpieczenia należytego wykonania umowy w formie gwarancji bankowej lub ubezpieczeniowej warunki przedmiotowej gwarancji będą zawierały następujące klauzule:

1. Gwarant zobowiązuje się nieodwołalnie i bezwarunkowo, na pierwsze pisemne żądanie Beneficjenta – Katowickiego Centrum Onkologii, do zapłaty na rzecz Beneficjenta kwoty do łącznej wysokości ......................złotych (słownie: ……………………………………….) z tytułu niewykonania lub nienależytego wykonania umowy,
2. żądaną należność Gwarant zapłaci Beneficjentowi w terminie 30 dni (słownie: trzydziestu dni) od dnia doręczenia Gwarantowi pisemnego wezwania do zapłaty zawierającego oświadczenie Beneficjenta, że żądana kwota jest należna,
3. wezwanie do zapłaty zostanie skierowane do Gwaranta bezpośrednio przez Beneficjenta lub   
   za pośrednictwem Banku Beneficjenta, który potwierdzi:
4. własnoręczność podpisów na wezwaniu,
5. uprawnienia do składania oświadczeń w imieniu Beneficjenta osób podpisujących wezwanie,
6. wskaże nr rachunku Beneficjenta, na który Gwarant powinien dokonać zapłaty z tytułu udzielonej gwarancji,
7. spory mogące wynikać z niniejszej gwarancji podlegają rozpoznaniu przez sąd właściwy dla siedziby Zamawiającego/Beneficjenta.

## Uwaga!

1. Gwarancja należytego wykonania umowy musi zawierać w sobie powyższą treść lub jej równoważne sformułowania.
2. Niedopuszczalne są w treści gwarancji niezdefiniowane określenia typu *„kompletne”* itp.
3. W przypadku wskazania szczegółowych wymogów formalnych niezbędna jest lista kontrolna umożliwiająca weryfikację kompletności wezwania.

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

**data, podpis i pieczątka osoby uprawnionej**

##### Załącznik Nr 6 do SIWZ

**................................................**

**Nazwa i adres Wykonawcy**

**Pieczątka firmowa**

**OŚWIADCZENIE O PODWYKONAWCACH**

**Oświadczam, że**

**\*** Wykonanie części zamówienia ……………………………………………………………………

(podać w jakim zakresie)

powierzam podwykonawcy/om …………………………………………………………………..

(podać komu – nazwa i adres firmy)

**\*** Całość zamówienia wykonam samodzielnie.

**Uwaga!**

**\* - niepotrzebne skreślić**

**…………………………………………………**

**data, podpis i pieczątka osoby uprawnionej**

##### Załącznik Nr 7 do SIWZ

**................................................**

Nazwa i adres Wykonawcy

**Pieczątka firmowa**

**KLAUZULA INFORMACYJNA z art. 13 RODO**

**w celu związanym z postępowaniem o udzielenie zamówienia publicznego**

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, informuję, że:

* administratorem Pani/Pana danych osobowych jest */* ***Katowickie Centrum Onkologii, ul. Raciborska 26, 40 – 074 Katowice, tel. 32 2511-761*** */;*
* inspektorem ochrony danych osobowych w */* ***Katowickie Centrum Onkologii*** */* jest Pan/Pani */****Tomasz Duniec****, kontakt:* ***IOD@kco.katowice.pl, tel. 32 42-00-290****/*;
* Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. cRODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego */* **zakup, dostarczenie i montaż wyposażenia serwerowni dla Katowickiego Centrum Onkologii***/* prowadzonym w trybie ***przetarg nieograniczony***;
* odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 1843), dalej „ustawa Pzp”;
* Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
* obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
* w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
* posiada Pani/Pan:

- na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;

- na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych;

- na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;

- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

* nie przysługuje Pani/Panu:

- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;

- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

- na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

**.………………………………………………**

**data, podpis i pieczątka osoby uprawnione**

***Załącznik Nr 8 do SIWZ***

**Umowa powierzenia przetwarzania danych osobowych**

zawarta w dniu ……………………… r. w Katowicach pomiędzy:

**Katowickie Centrum Onkologii**

40-074 Katowice, ul. Raciborska 26

KRS 0000096116, NIP 634-22-99-376, REGON 276201240.

zwanym dalej Zleceniodawcą lub Administratorem danych (administratorem)

reprezentowanym przez:

………………………………………………………………..

a

………………………………………………………………..

reprezentowanym przez:

………………………………………………………………..

zwanym dalej Zleceniobiorcą lub Podmiotem przetwarzającym.

zwanymi każdą z osobna w dalszej części Umowy „Stroną”, a łącznie „Stronami”.

Zważywszy, że:

1. Zleceniobiorca będzie wykonywał odpłatne świadczenie na rzecz Zleceniodawcy usług z zakresu wyłącznie w celu realizacji Umowy Głównej **………………………** w okresie niezbędnym dla jej realizacji.
2. Zleceniobiorca w ramach w/w usług będzie miał dostęp do danych kategorii osób, których dane dotyczą

a) Pacjenci Administratora Danych.

b) Personel Administratora Danych.

1. Zleceniobiorca w ramach w/w usług będzie miał dostęp do danych osobowych z kategorii osób Administratora danych, w zakresie:

a) Imię i nazwisko, płeć, data urodzenia, adres zamieszkania, PESEL, nr telefonu, e-mail, dane medyczne dot. pobytu pacjenta.

b) Imię i nazwisko, nr prawa wykonywania zawodu, PESEL, nr telefonu, e-mail.

1. Zakres danych osobowych wymienionych powyżej jest maksymalnym katalogiem danych, które mogą być przetwarzane w związku z realizacją Umowy. W rzeczywistości dane mogą być przekazywane przez Katowickie Centrum Onkologii w mniejszym zakresie bez uszczerbku dla postanowień Umowy. Zakres danych może ulec zmianie w przypadku zmiany aktualnie obowiązujących przepisów prawa.

Strony niniejszym postanawiają zawrzeć Umowę powierzenia przetwarzania danych osobowych

(„Umowa”), o następującej treści:

**§ 1**

**Definicje**

1. Podmiot przetwarzający – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora, zwany dalej Zleceniobiorcą

2. Administrator – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania, zwany dalej Zleceniodawcą,

3. Dane osobowe- oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,

4. Przetwarzanie- oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

5. Rozporządzenie- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

6. Inny podmiot przetwarzający - podmiot, któremu podmiot przetwarzający w imieniu administratora pod-powierzył w całości lub częściowo przetwarzanie danych osobowych.

**§ 2**

**Oświadczenia Stron**

1. Administrator danych i Zleceniobiorca oświadczają, że zawarli Umowę Głównej Nr **………………………..** w dniu **………………….**. na zakres usług zawartych w paragrafie 1 w/w Umowach w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 roku (zwanego dalej Rozporządzeniem) z tytułu, której będą wykonywane czynności w zakresie przetwarzania danych osobowych w zbiorze danych.

2. Niniejsza–akcesoryjna względem Umowy Głównej Nr **……………………** umowa powierzenia przetwarzania danych reguluje wzajemny stosunek stron i obowiązki w zakresie przetwarzania danych osobowych wynikających z zawartej w/w Umów.

3. Zleceniobiorca oświadcza, że dysponuje środkami (technicznymi i prawnymi, inne) umożliwiającymi prawidłowe przetwarzanie danych osobowych powierzonych przez Administratora danych, w zakresie i celu określonym Umową Główną Nr **……………………..** Rozporządzeniem oraz innymi przepisami prawa powszechnie obowiązującego.

4. Zleceniobiorca oświadcza również, że osobom zatrudnionym przy przetwarzaniu powierzonych danych osobowych nadane zostały upoważnienia do przetwarzania danych osobowych oraz że osoby te zostały zapoznane z przepisami o ochronie danych osobowych oraz z odpowiedzialnością za ich nieprzestrzeganie, zobowiązały się do ich przestrzegania oraz do bezterminowego zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczenia.

**§ 3**

**Obowiązki Zleceniobiorcy**

1. Zleceniobiorca zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Zleceniobiorca zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Zleceniobiorca zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Zleceniobiorca zobowiązuje się zapewnić zachowanie w tajemnicy,   
   (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Zleceniobiorca po zakończeniu świadczenia usług związanych z przetwarzaniem stosownie do decyzji Administratora usuwa lub zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. Zleceniobiorca pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Zleceniobiorca po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi, ale nie później niż w ciągu w ciągu 24 godzin.

**§ 4**

**Cel, zakres, miejsce przetwarzania powierzonych danych osobowych**

1. Administrator danych powierza Zleceniobiorcy przetwarzanie danych osobowych Administratora danych jedynie w celu prawidłowego wykonywania usługi opisanej szczegółowo w Umowie Głównej Nr **……………………..**

2. Zleceniobiorca zobowiązuje się do przetwarzania powierzonych danych osobowych wyłącznie w celach związanych z realizacją Umowy Głównej Nr **……………………….** i wyłącznie w zakresie, jaki jest niezbędny do realizacji tych celów.

3. Na wniosek Administratora danych lub osoby, której dane dotyczą Zleceniobiorca wskaże miejsca, w których przetwarza powierzone dane.

**§ 5**

**Zasady przetwarzania danych osobowych**

1. Strony zobowiązują się wykonywać zobowiązania wynikające z niniejszej Umowy z najwyższą starannością zawodową w celu zabezpieczenia prawnego, organizacyjnego i technicznego interesów Stron w zakresie przetwarzania powierzonych danych osobowych.

2. Zleceniobiorca zobowiązuje się zastosować środki techniczne i organizacyjne mające na celu należyte, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, zabezpieczenie powierzonych do przetwarzania danych osobowych, w szczególności zabezpieczyć je przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

3. Zleceniobiorca oświadcza, że zastosowane do przetwarzania powierzonych danych systemy informatyczne spełniają wymogi aktualnie obowiązujących przepisów prawa.

4. Zleceniobiorca przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora.

5. Podmiot przetwarzający, biorąc pod uwagę charakter przetwarzania, udziela informacji administratorowi w celu wywiązania się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw.

6. Podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych i aktów prawnych je implementujących oraz wykonujących) .

7. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora danych usuwa dane lub zwraca mu wszelkie dane osobowe. Jak również usuwa wszelkie ich istniejące kopie, chyba że szczególne przepisy prawa nakazują mu ich przechowywanie.

8. Podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszej umowie oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji.

9. Podmiot przetwarzający nie będzie korzystał z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora danych.

**§ 6**

**Prawo kontroli**

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Zleceniobiorcę przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Zleceniobiorcy i z minimum 2 dniowym uprzedzeniem o jej przeprowadzeniu.
3. Zleceniobiorca zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych, ale nie dłuższym niż 3 dni robocze.
4. Zleceniobiorca udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

**§7**

**Dalsze powierzenie danych do przetwarzania**

1. Zleceniobiorca może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Zleceniobiorcę prawo Unii lub prawo państwa członkowskiego, któremu podlega Zleceniobiorca. W takim przypadku przed rozpoczęciem przetwarzania Zleceniobiorca informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca Zleceniobiorcy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Zleceniobiorcę w niniejszej Umowie.
4. Zleceniobiorca ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

**§ 8**

**Odpowiedzialność**

1. Administrator danych ponosi odpowiedzialność za przestrzeganie przepisów prawa w zakresie przetwarzania i ochrony danych osobowych według rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

2. Powyższe nie wyłącza odpowiedzialności Zleceniobiorcy za przetwarzanie powierzonych danych niezgodnie z umową.

3. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem, jeśli nie dopełnił obowiązków, które nakłada niniejsza umowa, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom, a w szczególności Zleceniobiorca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, w tym za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.

4. Zleceniobiorca zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Zleceniobiorcę danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Zleceniobiorcy, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania u Zleceniobiorcy tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

**§9**

**Czas obowiązywania umowy**

Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas obowiązywania Umowy Głównej Nr **………………………………..**

**§10**

**Rozwiązanie umowy**

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:
   1. pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   2. przetwarza dane osobowe w sposób niezgodny z umową;
   3. powierzył przetwarzanie danych osobowych innemu podmiotowi bez wcześniejszej zgody Administratora danych.

**§11**

**Zasady zachowania poufności**

1. Zleceniobiorca zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Zleceniobiorca oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

**§12**

**Postanowienia końcowe**

1. Umowa powierzenia zastępuje dotychczasowe umowy powierzenia danych osobowych w zakresie powierzenia danych osobowych w związku z realizacją Umowy.
2. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
3. Wszelkie zmiany niniejszej Umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.
4. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia, jak również inne przepisy dotyczące ochrony danych osobowych, a także wszelkie nowelizacje, jakie wejdą w życie po dniu zawarcia Umowy, jak również akty prawne, które zastąpią wskazane ustawy i rozporządzenia.
5. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla Administratora danych.

Administrator danych Zleceniobiorca

**ANKIETA do Załącznika Nr 8 do SIWZ**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ANKIETA WYPEŁNIONA PRZEZ:  ….................................................................................................….......................................................................  – GWARANCJE WDROŻENIA ODPOWIEDNICH ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH PRZEZ PODMIOT PRZETWARZAJĄCY | | | | |  | |
| Niniejsza ankieta („Ankieta”) stanowi podstawę do oceny przez Administratora (dalej również: „ADO”), czy .................................................................................................., jako podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymagania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) („RODO”) i chroniło prawa osób, których dane dotyczą, w szczególności z uwzględnieniem kryteriów: fachowości, wiarygodności oraz zasobów.  Zakres Ankiety odpowiada wymogom określonym w RODO i stanowi kryteria wyboru podmiotu przetwarzającego opierające się w szczególności na: a) art. 28 ust. 1 RODO, zgodnie z którym „Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą”, oraz  b) motywie 81 RODO, zgodnie z którym: „Aby zapewnić przestrzeganie wymogów niniejszego rozporządzenia w przypadku przetwarzania, którego w imieniu administratora ma dokonać podmiot przetwarzający, administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania. Stosowanie przez podmiot przetwarzający zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji. | | | | |  | |
| L.p. | Pytanie | Odpowiedź (Tak/Nie) | Uwagi (dodatkowe informacje lub komentarz) |  | |
| 1 | Czy Organizacja posiada doświadczenie w świadczeniu usług związanych z powierzeniem przetwarzania danych? Jeśli tak, to jak długie? Prosimy o wykazanie doświadczenia w świadczeniu przedmiotowych usług (o ile to możliwe, wskazanie podmiotów, z którymi Organizacja współpracowała w ww. zakresie i czasie trwania współpracy). |  |  |  | |
| 2 | Czy Organizacja realizowała wcześniej umowy związane z powierzeniem przetwarzania danych osobowych? |  |  |  | |
| 3 | Czy Organizacja wdrożyła dokumentację opisującą zasady przetwarzania i ochrony danych osobowych? |  |  |  | |
| 4 | Czy przepisy RODO wymagają, aby Organizacja wyznaczyła inspektora ochrony danych? |  |  |  | |
| 5 | Czy Organizacja formalnie powołała inspektora ochrony danych i zgłosiła powołanie do inspektora Prezesa Urzędu Ochrony Danych Osobowych? |  |  |  | |
| 6 | W sytuacji braku powołania inspektora ochrony danych - czy zadania dotyczące zapewniania przestrzegania przepisów o ochronie danych osobowych w Organizacji pełnią inne osoby? |  |  |  | |
| 7 | Czy wyznaczone w Organizacji osoby do wykonywania w/w zadań posiadają odpowiednią wiedzę i przygotowanie praktyczne do wykonywania swoich obowiązków z tego zakresu? |  |  |  | |
| 8 | Czy Organizacja zamierza wyznaczyć inspektora danych osobowych, mimo że nie wymagają tego przepisy RODO lub też inną osobę/zespół odpowiedzialny za nadzór nad ochroną danych osobowych w Organizacji? Jeśli tak, to w jakim terminie? |  |  |  | |
| 9 | Czy osoby po stronie Organizacji dedykowane do obsługi administratora danych zostały przeszkolone i zapoznane w zakresie bezpieczeństwa informacji tym przepisów o ochronie danych osobowych? |  |  |  | |
| 10 | Czy przeprowadzane w Organizacji szkolenia w zakresie przepisów o ochronie danych osobowych zostały udokumentowane? (listy obecności, agenda szkolenia) |  |  |  | |
| 11 | Czy osoby zatrudnione w Organizacji przy przetwarzaniu danych zostały przeszkolone w zakresie obsługi administratora danych, w tym bezpiecznego korzystania z systemu informatycznego? |  |  |  | |
| 12 | Czy Organizacja posiada referencje od innych podmiotów, które obsługuje/obsługiwała w zakresie przetwarzania danych osobowych na ich zlecenie? |  |  |  | |
| 13 | Czy stwierdzono prawomocną decyzją PUODO lub innego organu nadzorczego lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez Organizację (odnosi się to również do poprzednika prawnego Organizacji)? |  |  |  | |
| 14 | Czy wobec Organizacji jest prowadzone lub było prowadzone jakiekolwiek postępowanie przez PUODO (wcześniej GIODO) i na jakim etapie jest sprawa lub jaką decyzję podjął organ nadzoru? |  |  |  | |
| 15 | Czy Organizacja opracowała i wdrożyła politykę ochrony danych lub podobny dokument zgodny z wymaganiami RODO? Jeżeli Organizacja nie posiada ww dokumentacji, to proszę o określenie w jakim terminie dokumentacja zostanie opracowana i wdrożona? |  |  |  | |
| 16 | Czy Organizacja opracowałą i wdrożyła procedurę obsługi żądań osób, których dane osobowe dotyczą (podmiotów danych)? Dotyczy procedur, którymi kieruje się kontrahent w odniesieniu do realizacji praw podmiotów danych zgodnie z art. 15-22 rodo. |  |  |  | |
| 17 | Czy Organizacja prowadzi rejestr czynności przetwarzania zgodnie z art. 30 rodo? |  |  |  | |
| 18 | Czy Organizacja prowadzi rejestr kategorii czynności przetwarzania zgodnie z art. 30 rodo? |  |  |  | |
| 19 | Czy Organizacja wdrożyła instrukcję lub podobny dokument określający zasady postępowania w sytuacji naruszenia ochrony danych osobowych? |  |  |  | |
| 20 | Czy Organizacja prowadzi ewidencję naruszeń przepisów o ochronie danych osobowych, w tym naruszeń bezpieczeństwa danych? |  |  |  | |
| 21 | Czy personel w Organizacji jest świadomy zagrożeń dla danych osobowych i obowiązku zgłoszenia podejrzenia naruszenia ochrony danych osobowych? |  |  |  | |
| 22 | Czy Organizacja wdrożyła zasady zarządzania bezpieczeństwem informacji, w tym: |  |  |  | |
| a) system zarządzania bezpieczeństwem informacji na podstawie normy ISO 27001? Czy posiada certyfikat? |  |  |  | |
| b) zasady zarządzania bezpieczeństwem informacji z elementami wykorzystania normy ISO 27002? |  |  |  | |
| 23 | Czy Organizacja wdrożyła inne zasady ochrony informacji – np. Polityka bezpieczeństwa informacji (wynikająca z normy ISO 27001)? |  |  |  | |
| 24 | Czy w Organizacji przeprowadzono szacowanie ryzyka uwzględniające ryzyko naruszenia praw lub wolności osób fizycznych wynikające z przetwarzania danych osobowych zgodnie z art. 32 rodo? |  |  |  | |
| 25 | Czy szacowanie ryzyka w Organizacji zostało udokumentowane, np. czy został stworzony plan postępowania z ryzykiem lub zakres zastosowania (Statement of Applicability)? |  |  |  | |
| 26 | Czy Organizacja dobrała zabezpieczenia zapewniające ochronę przetwarzanych danych osobowych adekwatnie do wyników szacowania ryzyka? |  |  |  | |
| 27 | Czy Organizacja okresowo przeprowadza kolejne działania związane z oszacowanym ryzykiem? |  |  |  | |
| 28 | Czy w przypadku zmiany poziomu ryzyka Organizacja dobiera nowe środki techniczne i organizacyjne zabezpieczające dane, stosownie do wyników analizy ryzyka? |  |  |  | |
| 29 | Czy występują operacje przetwarzania danych, dla których w Organizacji zidentyfikowano obecnie wysoki poziom ryzyka naruszenia praw lub wolności osób fizycznych? |  |  |  | |
| 30 | Czy dla planowanych operacji przetwarzania danych, dla których poziom ryzyka naruszenia praw lub wolności osób fizycznych oceniono jako wysoki Organizacja przewiduje dokonanie oceny skutków dla ochrony danych? |  |  |  | |
| 31 | Czy Organizacja prowadzi regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych, w celu weryfikacji spełniania wymogów polityki ochrony danych lub innej wewnętrznej procedury, w tym oceny skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania? |  |  |  | |
| 32 | Czy w ostatnim roku był przeprowadzany w Organizacji audyt w zakresie ochrony danych osobowych? |  |  |  | |
| 33 | Czy wnioski z audytów prowadzonych w Organizacji zostały udokumentowane, np. w raporcie audytowym? |  |  |  | |
| 34 | Czy personel Organizacji wyznaczony do realizacji umowy przetwarza dane osobowe wyłącznie z upoważnienia Administratora Danych Osobowych zgodnie z art. 29 rodo? Dotyczy formalnych upoważnień ze wskazanym zakresem i formą przetwarzania? Czy zostało to udokumentowane? |  |  |  | |
| 35 | Czy osoby upoważnione w Organizacji do przetwarzania danych w ramach realizacji umowy zostały obowiązane do zachowania ich w tajemnicy? Czy zostało to udokumentowane? |  |  |  | |
| 36 | Czy w Organizacji opracowano i wdrożono procedury dotyczące kontroli dostępu do danych w procesach przetwarzania danych osobowych? Dotyczy kontroli uprawnień w systemach informatycznych, dostępu do budynków i pomieszczeń, zakresu dostępu do dokumentacji w formie papierowej. |  |  |  | |
| 37 | Czy w związku z realizacją przedmiotu umowy dane osobowe są lub będą powierzane przez Organizację innym podmiotom tzw. podpowierzenie przetwarzania danych osobowych? |  |  |  | |
| 38 | Czy dane osobowe są przekazywane przez Organizację poza Europejski Obszar Gospodarczy? |  |  |  | |
| 39 | Czy w Organizacji dane osobowe są przetwarzane w systemach informatycznych? |  |  |  | |
| 40 | Czy systemy informatyczne służące do przetwarzania danych osobowych są administrowane przez personel Organizacji? |  |  |  | |
| 41 | Czy w Organizacji wdrożono procedury zapewnienia ciągłości działania systemów informatycznych służących do przetwarzania danych osobowych? Dotyczy sytuacji, w której dane osobowe są przetwarzane w systemie informatycznym? |  |  |  | |
| 42 | Czy w Organizacji dane osobowe przetwarzane na dyskach komputerów przenośnych są szyfrowane? |  |  |  | |
| 43 | Czy w Organizacji dane osobowe przetwarzane na nośnikach przenośnych np. pendrive, dysk zewnętrzny, są szyfrowane? |  |  |  | |
| Ankietę należy w terminie 7 dni, od dnia jej otrzymania wypełnić, podpisać i odesłać jej skan na adres poczty elektronicznej osoby do kontaktu po stronie Administratora danych. Ankietę uważa się za wypełnioną, jeśli na wszystkie pytania zostały udzielone odpowiedzi. Ankietę (w ilości egzemplarzy odpowiadającej ilości podmiotów występujących po stronie Administratora w umowie powierzenia) należy dołączyć w oryginale do umowy powierzenia. | | | | |  | |
| Podpisy osób upoważnionych do wypełnienia ankiety w imieniu Organizacji: | |  |  |  | |
|  | Imię i nazwisko: |  | |  | |
|  | Funkcja/Stanowisko: |  | |  | |
|  | Data: |  | |  | |
|  | Podpis: |  | |  | |