DZP/381/25/EIN/2018 Katowice 07.06.2018r.

ZAPROSZENIE DO SKŁADANIA OFERT

(do niniejszego postępowania nie stosuje się ustawy Prawo zamówień publicznych, gdyż wartość szacunkowa zamówienia nie przekracza wyrażonej w złotych równowartości kwoty 30 000 euro)

1. **Zamawiający:** Uniwersyteckie Centrum Kliniczne im. prof. K. Gibińskiego Śląskiego Uniwersytetu Medycznego w Katowicach, 40-514 Katowice, ul. Ceglana 35 zaprasza do składania ofert na**: Dostawę sprzętu komputerowego.**

   Wyszczególnienie ilościowe przedmiotu zamówienia określa formularz asortymentowo-cenowy (załącznik nr 2 do niniejszego zaproszenia).
   Szczegółowy opis przedmiotu zamówienia określa Zestawienie Parametrów Technicznych (załącznik nr 3 do niniejszego zaproszenia).
   Szczegółowe warunki realizacji dostaw zawiera projekt umowy (załącznik nr 4 do niniejszego zaproszenia).

2. **Oferta powinna zawierać:**

   1) Wypełniony czytelnie, podpisany i opieczętowany przez osobę uprawnioną/ osoby uprawnione do reprezentowania Wykonawcy formularz ofertowy według druku stanowiącego załącznik nr 1 do niniejszego zaproszenia.
   2) Wypełniony czytelnie, podpisany i opieczętowany formularz asortymentowo - cenowy stanowiący załącznik nr 2.
   3) Wypełnione czytelnie, podpisane i opieczętowane Zestawienie Parametrów Technicznych stanowiące załącznik nr 3
   4) Pełnomocnictwo osoby lub osób podpisujących ofertę, jeżeli nie wynika to bezpośrednio z załączonych dokumentów.
      UWAGA: w przypadku nie dołączenia do oferty w/w dokumentów oferta Wykonawcy będzie podlegać odrzuceniu

3. **Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami oceny ofert:**

   a) Cena – 75 %,
   b) Termin dostawy – 25 %;

kryterium Cena (C) – waga 75%

W ramach kryterium „Cena" ocena ofert zostanie dokonana przy zastosowaniu wzoru:

$$C = \frac{Cn}{Co} \times 100 \times 75\ \%$$

gdzie:
C – liczba punktów w ramach kryterium „Cena",
Cn - najniższa cena spośród ofert ocenianych
Co - cena oferty ocenianej

Ocenie w ramach kryterium „Cena" podlegać będzie cena łączna brutto za wykonanie całego przedmiotu zamówienia podana w formularzu asortymentowo-cenowym.
W tym kryterium wykonawca może uzyskać maksymalnie 75 punktów.

kryterium termin dostawy (TD) – waga 25%
Sposób obliczania punktów dla w/w kryterium:
TD – liczba punktów w ramach kryterium „termin dostawy”

Termin dostawy	Liczba punktów
1 – 10 dni kalendarzowych od dnia zawarcia umowy	25
11- 15 dni kalendarzowych od dnia zawarcia umowy	15
16- 20 dni kalendarzowych od dnia zawarcia umowy	5
21 -30 dni kalendarzowych od dnia zawarcia umowy	0

Sposób obliczenia punktów dla w/w kryterium:

1. Kryterium termin dostawy będzie rozpatrywane na podstawie zadeklarowanego w formularzu ofertowym terminu dostawy. Termin ten będzie liczony od dnia zawarcia umowy.
2. Termin dostawy nie może być dłuższy niż 30 dni kalendarzowych od dnia zawarcia umowy
3. Maksymalna liczba punktów jaką można uzyskać w tym kryterium to 25 punktów.
4. Jeżeli wykonawca wpisze termin dostawy dłuższy niż 30 dni kalendarzowych to przygotuje ofertę niezgodną z zaproszeniem co skutkować będzie odrzuceniem oferty. W przypadku nie wypełnienia w formularzu ofertowym stosownej rubryki zamawiający uzna, że wykonawca deklaruje najdłuższy termin dostawy tj. 30 dni kalendarzowych.

Za najkorzystniejszą ofertę zostanie uznana oferta, która uzyskała łącznie najwyższą liczbę punktów obliczoną wg następującego wzoru:

P= C+ TD

gdzie:

P - łączna liczba punktów jaką uzyskała oceniana oferta
C - liczba punktów przyznanych ocenianej ofercie w ramach kryterium cena
TD - liczba punktów przyznanych ocenianej ofercie w ramach kryterium termin dostawy

4. **Miejsce i termin składania ofert –** Uniwersyteckie Centrum Kliniczne im. prof. K. Gibińskiego Śląskiego Uniwersytetu Medycznego w Katowicach, ul. Ceglana 35 40-514 Katowice, Sekretariat – pokój D021 – w terminie do dnia 12.06.2018 r. do godz. 12:00

Ofertę należy złożyć w zamkniętej, opisanej według poniższego wzoru kopercie:

„ Nazwa, adres Wykonawcy
.....
Uniwersyteckie Centrum Kliniczne
im. prof. K. Gibińskiego
Śląskiego Uniwersytetu Medycznego w Katowicach
ul. Ceglana 35 40-514 Katowice
„Oferta na dostawę sprzętu komputerowego

– Nie otwierać przed ……., godz.12:00”

5. 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 uzyskanych w niniejszym postępowaniu danych osobowych jest Uniwersyteckie Centrum Kliniczne im. prof. K. Gibińskiego Śląskiego Uniwersytetu Medycznego w Katowicach, 40-514 Katowice, ul. Ceglana 35, Tel. 32 3581200 fax. 32 251-84-37 lub 32/358-14-32, adres strony www: https://www.uck.katowice.pl/
- inspektorem ochrony danych w Uniwersyteckim Centrum Kliniczne im. prof. K. Gibińskiego Śląskiego Uniwersytetu Medycznego w Katowicach jest Pan Patryk Rozumek *tel.* 32 3581 433, iod@uck.katowice.pl
- uzyskane w niniejszym postępowaniu dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem pn. **„Dostawa sprzętu komputerowego " - DZP/381/25/EIN/2018**
- odbiorcami uzyskanych w niniejszym postępowaniu danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja zgodnie z wymaganiami prawa powszechnego
- uzyskane w niniejszym postepowaniu dane osobowe będą przechowywane, przez okres 5 lat od dnia zakończenia postępowania
- obowiązek podania danych osobowych bezpośrednio dotyczących danej osoby jest wymogiem ustawowym określonym w przepisach kodeksu
- w odniesieniu do uzyskanych w postępowaniu danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- osoba, której dane osobowe dotyczą posiada:
  - na podstawie art. 15 RODO prawo dostępu do danych osobowych jej dotyczących;
  - na podstawie art. 16 RODO prawo do sprostowania danych osobowych jej dotyczących (Wyjaśnienie: skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania ani zmianą postanowień umowy w zakresie niezgodnym z wymaganiami prawa powszechnie obowiązującego);
  - 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 (**Wyjaśnienie:** prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego);
  - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy osoba, której dane osobowe dotyczą uzna, że przetwarzanie jej danych osobowych narusza przepisy RODO;
- nie przysługuje osobie, której dane osobowe dotyczą:
  - 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 tych danych osobowych jest art. 6 ust. 1 lit. c RODO**.

6. Osoba uprawniona do porozumiewania się z wykonawcami:
Ewa Kamzela Dział Zamówień Publicznych pok. E055 tel. 32 3581-445
e-mail: bzp@uck.katowice.pl w godzinach pracy tj. od poniedziałku do piątku w godz. 7.25 – 15.00.

Zapraszający zastrzega sobie prawo do nie dokonania wyboru Wykonawcy bez podania przyczyn.

Załączniki:
1. Formularz ofertowy
2. Formularz asortymentowo-cenowy
3. Zestawienie Parametrów Technicznych
4. Projekt umowy

Z upoważnienia Dyrektora
Uniwersyteckiego ... prof. K. Gibińskiego
Śląskiego Uniwersytetu Medycznego w Katowicach
mgr ... Kierownik Działu Zamówień Publicznych

.....
pieczęć firmowa wykonawcy

FORMULARZ OFERTOWY
DLA UNIWERSYTECKIEGO CENTRUM KLINICZNEGO im. Prof. K. Gibińskiego
ŚLĄSKIEGO UNIWERSYTETU MEDYCZNEGO W KATOWICACH

Nazwa Wykonawcy .....

Siedziba: .....

Adres zamieszkania*……
**) dotyczy osób fizycznych prowadzących działalność gospodarczą oraz wspólników w spółce cywilnej*

REGON ..... NIP .....

Tel. ..... fax .....

strona www ..... e-mail .....

Osoba wskazana do kontaktu z Zamawiającym .....

1. W odpowiedzi na zaproszenie do złożenia oferty na **dostawę sprzętu komputerowego** oferujemy realizację przedmiotowego zamówienia za maksymalną łączną kwotę określoną w dołączonym formularzu asortymentowo-cenowym.
2. **Oświadczamy, iż oferujemy następujący termin dostawy:** …… dni kalendarzowych od dnia zawarcia umowy *(należy wpisać oferowaną ilość dni - maksymalnie 30. W przypadku nie uzupełnienia Zamawiający przyjmuje, iż Wykonawca oferuje termin dostawy 30 dni kalendarzowych od dnia zawarcia umowy.)*

4. Oświadczamy, ze uważamy się związani z niniejszą ofertą przez okres 30 dni.
3. Oświadczamy, że zawarta w Zaproszeniu treść projektu umowy została przez nas zaakceptowana i zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy na wyżej wymienionych warunkach w miejscu i terminie wyznaczonym przez Zamawiającego.
4. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 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) (dalej w treści RODO) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia w niniejszym postępowaniu.*
   ***W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO, może wykreślić treść niniejszego oświadczenia)**

.....

podpis i pieczęć osoby uprawnionej/osób uprawnionych

do reprezentowania wykonawcy

FORMULARZ ASORTYMENTOWO-CENOWY
WYSZCZEGÓLNIENIE ASORTYMENTOWE I ILOŚCIOWE PRZEDMIOTU ZAMÓWIENIA

Lp.	Nazwa	J.m.	Ilość	Cena jednostkowa netto	Wartość netto (ilość x cena jednostkowa netto)	VAT %	Wartość brutto (wartość netto + VAT)
1	Zestaw komputerowy o parametrach opisany w Zestawieniu Parametrów Technicznych	Szt.	10				
				RAZEM:		**X**	

W pozycji VAT % dopuszcza się wpisanie zamiennie liczbowej lub procentowej wartości stawki podatku VAT

.....
podpis i pieczęć osoby uprawnionej/osób uprawnionych
do reprezentowania wykonawcy

ZESTAWIENIE PARAMETRÓW TECHNICZNYCH

Dostawa sprzętu komputerowego– ilość 10 kompletów SFF

Przedmiot zamówienia należy dostarczyć do lokalizacji Ceglana

Lp.	Wymagania minimalne	**Wymagana wartość**	**Wartość oferowana przez Wykonawcę**
1	**Przeznaczenie zestawów komputerowych:**		
a	Praca sieciowa w aplikacji bazodanowej z wykorzystaniem m.in. aplikacji webowych	TAK	TAK/NIE*
b	Praca na aplikacjach biurowych, m.in. pakiet Microsoft Office w wersji od 2010 w wzwyż, pakiet Open Office w wersji 4.x, pakiet Libre Office 5.x	TAK	TAK/NIE*
c	Praca z wykorzystaniem popularnych przeglądarek internetowych m.in. Internet Explorer w wersji 10 i w wzwyż, Mozilla Firefox w wersji 47.x i w wzwyż	TAK	TAK/NIE*
2	**Wymagane parametry techniczne dla komputerów:**		
a	Pamięć operacyjna minimum 16GB typu DDR4 (w jednej kości) z możliwością rozbudowy do 64GB tylko poprzez dołożenie kolejnych modułów pamięci	TAK	TAK/NIE* podać pojemność pamięci operacyjnej: ……
b	Interfejs sieciowy Ethernet 10/100/1000BaseTX, złącze RJ45	TAK	TAK/NIE* podać model lub inne wskazanie umożliwiające na jednoznaczną identyfikację produktu: ……..
c	Karta graficzna pracująca w trybie Full HD, wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA, obsługująca DirectX 12, OpenGL 4.x, możliwość osiągnięcia rozdzielczości 4096x2304pikseli (DP) oraz 1920x1080pikseli (VGA), umożliwiająca obsługę minimum 2 monitorów jednocześnie	TAK	TAK/NIE* podać model lub inne wskazanie umożliwiające na jednoznaczną identyfikację produktu: ……..
d	Pamięć masowa o pojemności minimum 128GB typu SSD, z partycją RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii	TAK	TAK/NIE* podać pojemność: ……
e	Płyta główna w pełni dopasowana do pozostałych elementów komputera, kompatybilna z zainstalowanymi elementami jednostki centralnej, wyposażona w chipset dedykowany do zainstalowanego procesora i pamięci operacyjnej tak by nie ograniczać możliwości tychże podzespołów, wyposażona minimum w 3 złącza SATA 6Gb/s, wyposażona w minimum 2 banki do obsługi pamięci operacyjnej minimum DDR4-2133,	TAK	TAK/NIE*

f	Procesor typu x86 z pamięcią podręczną nie mniejszą niż 6MB	TAK	TAK/NIE*
g	Zintegrowana karta dźwiękowa, zgodna z HD Audio	TAK	TAK/NIE*
h	Napęd optyczny DVD-RW wraz z oprogramowaniem do odtwarzania i nagrywania - do zastosowań w celach komercyjnych	TAK	TAK/NIE* Podać nazwę programowania lub inne wskazanie umożliwiające na jednoznaczną identyfikację produktu: ……..
i	Zasilacz o sprawności energetycznej powyżej 80% (certyfikat 80 PLUS Bronze – logo jednostki certyfikującej uwidocznione na tabliczce znamionowej zasilacza), zgodny z normą ENERGY STAR 6.0, mocy nie większej niż 300W.	TAK	TAK/NIE*
3	**Wymagana funkcjonalność dla komputerów:**		
a	Wydajność obliczeniowa komputera na podstawie testów aplikacyjnych SYSmark2014 (www.bapco.com): w teście SYSmark 2014 Overall minimum 1700 pkt, w teście SYSmark 2014 Office Productivity minimum 1300 pkt, w teście SYSmark 2014 Data/Financial Analysis minimum 1960 pkt.	TAK	TAK/NIE* Podać model, oznaczenie oferowanego procesora model lub inne wskazanie umożliwiające na jednoznaczną identyfikację produktu: ……..
b	Obudowa typu SFF (small form factor) z obsługą kart PCI Express wyłącznie o niskim profilu (minimum 1 x PCI-e 3.0 x16 oraz minimum 1 x PCI-e 2.0 x1). Obudowa wyposażona w minimum dwie kieszenie: (1 szt 5,25" (dopuszcza się w wersji tzw slim zajętej przez napęd optyczny oraz 1 szt 3,5" umożliwiającą rozbudowę komputera do konfiguracji dwudyskowej w oparciu o dyski 2,5" lub 3,5" lub w zamian złącze M.2). Obudowa musi być wyposażona w filtr przeciw pyłkowy zapobiegający nadmiernemu gromadzeniu się kurzu w środku obudowy. Obudowa musi umożliwiać bez narzędziową, wymianę dysków i kart rozszerzających. Obudowa trwale oznaczona nazwą komputera, numerem katalogowym, numerem seryjnym umożliwiającymi jednoznaczne, bez problemowe identyfikowanie sprzętu w całym okresie jego eksploatacji przez Zamawiającego. Obudowa musi posiadać dedykowane oczko na kłódkę umożliwiającą zastosowanie zabezpieczenia fizycznego przed otwarciem obudowy. Obudowa przystosowana do pracy w pionie i poziomie.	TAK	TAK/NIE*
c	Zgodność z systemami operacyjnymi i standardami potwierdzona certyfikatem WHCL oraz certyfikatem CE	TAK	TAK/NIE*
d	Złącza zewnętrzne minimum: słuchawkowe, mikrofonowe, USB 2.0 2 sztuki, USB 3.0 4 sztuki, RJ45 1 sztuka, DisplayPort 1 sztuka, port RS232 1szt, wymagana ilość portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.	TAK	TAK/NIE*
e	BIOS zgodny ze specyfikacją UEFI	TAK	TAK/NIE*

f	Możliwość odczytania z BIOS: (wersji BIOS, modelu procesora wraz z informacjami o ilości rdzeni, prędkościach min i max zegara, wielkości podręcznej pamięci Cache, informacji o ilości pamięci RAM, informacji o dysku twardym)	TAK	TAK/NIE*
g	Możliwość wyłączenia zintegrowanej(nych) karty sieciowej, możliwość wyłączenia portów USB z poziomu BIOS bez uruchamiania systemu operacyjnego komputera	TAK	TAK/NIE*
h	Funkcja blokowania/odblokowywania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego	TAK	TAK/NIE*
i	Możliwość ustawienia hasła na poziomie administratora bez potrzeby uruchamiania systemu operacyjnego	TAK	TAK/NIE*
j	Nie dopuszcza się stosowania tzw. overclockingu w celu uzyskania wymaganych parametrów pracy zestawu komputerowego	TAK	TAK/NIE*
k	System diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: - testu pamięci RAM, - testu dysku twardego, - testu monitora, - testu magistrali PCI-e, - testu portów USB, - testu płyty głównej. Sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera.	TAK	TAK/NIE* Podać formę sygnalizacji błędów: np. (świetlna, dźwiękowa, inna) ……
4	**Wyposażenie dodatkowe komputerów:**		
a	Zainstalowany system operacyjny w wersji do zastosowań komercyjnych, profesjonalnych, interfejs systemu w języku polskim, wg wymagań **wyszczególnionych w uwadze nr 1 pod niniejszym zestawieniem parametrów technicznych** z licencją dożywotnią	TAK	TAK/NIE* Podać nazwę, wersję oferowanego oprogramowania lub inne wskazanie umożliwiające na jednoznaczną identyfikację zaoferowanego oprogramowania: ……
b	Zainstalowany pakiet antywirusowy (10 licencji dla komputerów przeznaczonych do dostarczenia do lokalizacji Ceglana) w wersji do zastosowań komercyjnych, profesjonalnych wg wymagań **wyszczególnionych w uwadze nr 2 pod niniejszym zestawieniem parametrów technicznych**	TAK	TAK/NIE* Podać nazwę, wersję oferowanego oprogramowania lub inne wskazanie umożliwiające na jednoznaczną identyfikację zaoferowanego oprogramowania: ……

c	Przewodowa klawiatura USB w układzie polski programisty/US. Długość przewodów minimum 140cm.	TAK	TAK/NIE*
d	Przewodowa mysz optyczna USB z minimum dwoma przyciskami i rolka (scroll). Długość przewodów minimum 140cm.	TAK	TAK/NIE*
5	**Warunki gwarancji dla komputerów:**		
a	Gwarancja	minimum 36 miesięcy	podać: ……
b	W przypadku awarii dysku twardego jak i komputera dysk pozostaje u Zamawiającego	TAK	TAK/NIE* ……
c	Serwis musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta	TAK	TAK/NIE* Nazwa …….. Siedziba……..
d	Należy wskazać numer telefoniczny i adres email dla wsparcia technicznego i informacji produktowej	podać	Tel:..... e-mail ……..….
e	Producent musi umożliwiać poprzez stronę internetową: - weryfikację modelu komputera, - weryfikację posiadanej/wykupionej gwarancji, - weryfikację statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego	TAK	TAK/NIE*
f	Czas usunięcia uszkodzenia w okresie gwarancji do 14 dni roboczych od momentu pisemnego zgłoszenia awarii, sprzęt do naprawy i z naprawy Wykonawca dostarcza na swój koszt	TAK	TAK/NIE*
g	Dostarczony sprzęt musi być fabrycznie nowy, nie starszy niż 6 miesięcy od daty produkcji	TAK	TAK/NIE*
Należy podać nazwę producenta, typ, model, numer katalogowy lub inne wskazanie ofertowanego sprzętu umożliwiające jednoznaczną identyfikację komputera: **……**			
6	**Minimalne wymagania dla monitorów:**		
a	Monitor musi posiadać możliwość montażu na ścianie z wykorzystaniem otworów montażowych w standardzie VESA 100, z możliwością bez narzędziowego demontażu stopy	TAK	TAK/NIE*
b	Ekran o przekątnej minimum 21,5 cali, WLED, TFT VA, matowy	TAK	TAK/NIE*
c	Rozdzielczość minimum Full HD 1920x1080 pikseli	TAK	TAK/NIE*
d	Wielkość plamki (pojedynczego piksela) maksymalnie 0,248mm	TAK	TAK/NIE*
e	Kontrast minimum 1000:1 (typowy)	TAK	TAK/NIE*
f	Jasność wyświetlacza nie mniejsza niż 250cd/m2	TAK	TAK/NIE*
g	Gniazda wejściowe: D-Sub (VGA),DP	TAK	TAK/NIE*

h	Waga monitora do 4kg	TAK	TAK/NIE*
i	Monitor musi posiadać możliwość regulacji pochylenia w zakresie minimum 27 stopni	TAK	TAK/NIE*
j	Monitor musi być wyposażony we wszystkie niezbędne kable przyłączeniowe m.in. kabel DisplayPort, kabel zasilający	TAK	TAK/NIE*
k	Obudowa monitora oznaczona nazwą producenta, numerem seryjnym i katalogowym pozwalającym na jednoznaczne identyfikowanie zaoferowanego monitora	TAK	TAK/NIE*
l	Maksymalne zużycie energii nie może przekraczać 25W, a w trybie czuwania nie więcej niż 0,5W	TAK	TAK/NIE*
m	Monitor musi posiadać minimum certyfikaty: Energy Star 6.0 i EPEAT Gold (potwierdzoną na stronie www.epeat.net), TCO i deklarację RoHS	TAK	TAK/NIE*
7	**Warunki gwarancji dla monitorów:**		
a	Gwarancja od momentu podpisania Protokołu Odbioru	minimum 36 miesięcy	Podać ….
b	Serwis musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta	TAK	TAK/NIE* Nazwa…… Siedziba……
c	Należy wskazać numer telefonu i adres email dla wsparcia technicznego i informacji produktowej	podać	Tel:..... e-mail ……
d	Producent musi umożliwiać poprzez stronę internetową: - weryfikację modelu monitora, - weryfikację posiadanej/wykupionej gwarancji, - weryfikację statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego	TAK	TAK/NIE*
e	Czas usunięcia uszkodzenia do 14 dni roboczych od momentu pisemnego zgłoszenia awarii, sprzęt do naprawy i z naprawy Wykonawca dostarcza na swój koszt	TAK	TAK/NIE*
f	Dostarczony sprzęt musi być fabrycznie nowy, nie starszy niż 6 miesięcy od daty produkcji	TAK	TAK/NIE*
Należy podać nazwę producenta, typ, model, numer katalogowy lub inne wskazanie ofertowanego sprzętu umożliwiające jednoznaczną identyfikację monitora: ……			

UWAGA nr 1 (dotyczy punktu 4 a Zestawienia Parametrów Technicznych)

Minimalne wymagania dla systemu operacyjnego zainstalowanego na komputerach objętych niniejszym zamówieniem

Lp.	Wymagania minimalne systemu operacyjnego
1	Wymagania dla systemu 64bit:
a	Nie wymaga aktywacji za pomocą telefonu lub Internetu u producenta
b	Licencja dożywotnia użytkownika
c	Poprawna obsługa pamięci operacyjnej w ilości powyżej 4GB

2	System musi spełniać następujące wymagania poprzez natywne dla niego mechanizmy, bez użycia dodatkowych aplikacji:
a	możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat); internetowa aktualizacja zapewniona w języku polskim; wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IPv4 i IPv6; zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi); funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer; interfejs użytkownika działający w trybie graficznym z elementami 3D; zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta; możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników; zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych; zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych; funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego; funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika; zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi; wbudowany system pomocy w języku polskim; możliwość przystosowania stanowiska dla osób niepełnosprawnych (i słabo widzących);
b	możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; wsparcie dla logowania przy pomocy smartcard; rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; system posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; wsparcie dla Sun Java i .NET Framework 1.1, 2.0, 3.0 i 4.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; wsparcie dla Jscript i VBScript – możliwość uruchamiania interpretera poleceń; zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami (obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową); rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację; graficzne środowisko instalacji i konfiguracji; transakcyjny system plików pozwalający na stosowanie przydziałów na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe; udostępnianie modemu; oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; możliwość przywracania plików systemowych; system operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.); możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (i przy użyciu numerów identyfikacyjnych sprzętu);
c	Pełna integracja z domeną Active Directory MS Windows (posiadaną przez Zamawiającego) opartą na serwerach Windows Server 2012R2; zarządzanie komputerami poprzez Zasady Grup (GPO) Active Directory MS Windows (posiadaną przez Zamawiającego), WMI; pełna obsługa ActiveX;
3	Współpraca z posiadanymi aplikacjami:
a	ze względu na posiadane przez Zamawiającego oprogramowanie Microsoft Office 2003/2007/2010/2013/2016 wymagana jest możliwość instalacji tego oprogramowania na systemie operacyjnym oferowanym przez Wykonawcę
b	ze względu na posiadaną przez Zamawiającego aplikację bazodanową InfoMedica (firmy Asseco Poland S.A.) wymagana jest możliwość instalacji tego oprogramowania na systemie operacyjnym oferowanym przez Wykonawcę. Dostarczone komputery będą wykorzystane do pracy z systemem AMMS (firmy Asseco Poland), który korzysta z przeglądarki internetowej, wtyczki Java, Wtyczki Flash.
c	zaoferowany system operacyjny będzie mógł być wykorzystywany (bez konieczności wykonywania jakichkolwiek modyfikacji) w sieciach informatycznych do przetwarzania informacji wrażliwych (dane osobowe, dane medyczne, dane finansowe)

4	Możliwość wykonania downgrad'u (zmiany wersji na niższą) w ramach posiadanej licencji (bez konieczności posiadania/dokupowania dodatkowej licencji na obniżaną wersję systemu)

UWAGA nr 2: (dotyczy punktu 4 b Zestawienia Parametrów Technicznych)

Minimalne wymagania dla systemu pakietu bezpieczeństwa zainstalowanego na komputerach objętych niniejszym zamówieniem

Zamawiający obecnie posiada pakiet antywirusowy ESET Endpoint Security Suite (**373** licencji w lokalizacji Ceglana ważnych do 5.09.2020r) wraz z wdrożoną konsolą do centralnego zarządzania Oprogramowanie to będzie używane na dostarczonych komputerach

1. Udzielona licencja powinna umożliwić użytkowanie programu we wszystkich jednostkach organizacyjnych Zamawiającego.
2. Użyte przez Zamawiającego wszelkie nazwy handlowe, znaki towarowe, patenty i miejsce pochodzenia są uzasadnione specyfiką przedmiotu zamówienia i mają na celu wskazanie jedynie jakości przedmiotu zamówienia.
3. W przypadku zaoferowania ESET Endpoint Security Suite, zamawiający wymaga, by licencja była dostarczona w formie rozszerzenia klucza dla **373** licencji przytoczonych powyżej, o ilość równą ilości zamawianych komputerów dla lokalizacji Ceglana **tj. 10 licencji z okresem ważności jak posiadany klucz przez Zamawiającego.**
4. W przypadku zaoferowania innego pakietu antywirusowego niż obecnie posiadany przez Zamawiającego wymaga się, aby współpracował on z konsolą centralnego zarządzania posiadaną i wdrożoną przez Zamawiającego Eset Remote Administrator Console. Poniżej Zamawiający wskazuje wymagania minimalne dla pakietu antywirusowego:

1	***Wymagania ogólne dla stacji roboczych:*** • Pełne wsparcie dla systemu Windows Vista/Windows 7/Windows 8/8.1/Windows 10 • Wsparcie dla 32 i 64-bitowej wersji systemu Windows lub innego dostarczonego razem z komputerami • Wersja programu dostępna w całości w języku polskim • Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim • Skuteczność programu potwierdzona nagrodami VB100 i co najmniej dwie inne niezależne organizacje takie jak ICSA Labs lub Check Mark
2	***Ochrona antywirusowa i antyspyware:*** • Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. • Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. • Wbudowana technologia do ochrony przed rootkitami. • Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. • Możliwość skanowania całego dysku, dysków sieciowych oraz nośników zewnętrznych wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. • System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak - nie wykonywało danego zadania. • Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami, (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). • Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. • Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu. • Skanowanie plików spakowanych i skompresowanych. • Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń). • Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. • Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. • Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. • W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany

	o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. • Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. • Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. • Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). • Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym. • Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie. • Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. • Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. • Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony. • Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora. • Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. • Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie. • Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. • Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. • Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego. • Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. • Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym. • Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. • W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne. • Wbudowane dwa niezależne moduły heurystyczne - jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie - z użyciem jednej i/lub obu metod jednocześnie. • Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. • Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. • Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. • Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. • Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. • Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik komputera przy próbie dostępu do konfiguracji był proszony o podanie hasła. • Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło. • Możliwość zabezpieczenia hasłem konfiguracji programu oraz jego nieautoryzowanej próby

	deinstalacji • Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji - poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji. • Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. • Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów. • System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. • Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych • Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. • Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia. • Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. • W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. • Użytkownik ma posiadać możliwość takiej konfiguracji aplikacji aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika • Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). • Moduł HIPS musi posiadać możliwość pracy w jednym z czterech trybów: • tryb automatyczny z regułami gdzie aplikacja automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to aplikacja pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym aplikacja uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu aplikacja musi samoczynnie przełączyć się w tryb pracy oparty na regułach. • Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. • Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. • Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach. • Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. • Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. • Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami. • Aplikacja musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. • Aplikacja musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http • Aplikacja musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback). • Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa). • Program ma wspierać technologię CISCO NetWork Access Control.

	• Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania. • W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór następujących modułów do instalacji: ochrona antywirusowa i antyspywerowa, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, kopia dystrybucyjna
3	***Ochrona przed spamem:*** • Ochrona antyspamowa dla różnych programów pocztowych wykorzystująca filtry Bayes-a, białą i czarną listę oraz bazę charakterystyk wiadomości spamowych. • Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. • Integracja z różnymi programami pocztowymi - antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego. • Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. • Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym. • Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam. • Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam. • Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana" oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana". • Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

4	***Zapora osobista (personal firewall):***
	• Zapora osobista ma pracować jednym z 5 trybów:
	  • tryb automatyczny - program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące,
	  • tryb automatyczny z wyjątkami - działa podobnie jak tryb automatyczny, ale umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł,
	  • tryb interaktywny - program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo),
	  • tryb oparty na regułach - użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany,
	  • tryb uczenia się - umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji.
	• Możliwość tworzenia list sieci zaufanych.
	• Możliwość dezaktywacji funkcji zapory sieciowej na kilka sposobów: pełna dezaktywacja wszystkich funkcji analizy ruchu sieciowego, tylko skanowanie chronionych protokołów oraz dezaktywacja do czasu ponownego uruchomienia komputera.
	• Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
	• Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję.
	• Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń.
	• Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.
	• Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.
	• Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
	• Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.
	• Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
	• Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
	• Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu

	danej sieci • Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora. • Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, aktywności wyłącznie jednego połączenia sieciowego lub wielu połączeń sieciowych konkretny interfejs sieciowy w systemie. • Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6 • Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci. • Możliwość aktualizacji sterowników zapory osobistej po restarcie komputera.
5	***Kontrola dostępu do stron internetowych:*** • Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych. • Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły. • Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego. • Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika. • Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i pod kategorii. • Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. • Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta. • Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.

DZP/381/25/EIN/2018 Załącznik nr 4

(Projekt)

UMOWA nr …….

(do niniejszej umowy nie stosuje się ustawy Prawo zamówień publicznych, gdyż wartość szacunkowa zamówienia nie przekracza wyrażonej w złotych równowartości kwoty 30.000,00 euro)

zawarta w dniu ..... w Katowicach
Strony umowy:

Zamawiający: – Uniwersyteckie Centrum Kliniczne im. prof. K. Gibińskiego Śląskiego Uniwersytetu Medycznego w Katowicach, 40-514 Katowice, ul. Ceglana 35
KRS 0000049660, NIP 954-22-74-017, REGON 001325767
reprezentowane przez:
Dyrektora – Ireneusza Ryszkiel
oraz

Wykonawca: ……

§1
PRZEDMIOT UMOWY

1. Wykonawca zobowiązuje się sprzedać i dostarczyć, a Zamawiający zobowiązuje się nabyć sprzęt komputerowy w ilości wskazanej w załączniku nr 1 oraz o parametrach opisanych w załączniku nr 2 do niniejszej umowy zwany dalej sprzętem.
2. Wykonawca oświadcza i gwarantuje, że dostarczony sprzęt jest:
   a) fabrycznie nowy, kompletny, zdatny i dopuszczony do obrotu i używania,
   b) wolny od wad fizycznych i prawnych;
   c) został wyprodukowany z zachowaniem najwyższych standardów jakości;

3. Wykonawca oświadcza i gwarantuje, że udzielając licencji na korzystanie z oprogramowania zainstalowanego w dostarczanym sprzęcie komputerowym nie narusza żadnych praw osób trzecich oraz nie zachodzą jakiekolwiek podstawy do zgłoszenia przez osoby trzecie roszczeń do tych praw.

§2
WARUNKI REALIZACJI UMOWY

1. Wykonawca zobowiązuje się dostarczyć sprzęt do siedziby Zamawiającego, w terminie do ……. dni od dnia podpisania umowy.
2. O przewidywanym terminie odbioru Wykonawca zawiadomi Zamawiającego, z co najmniej 1- dniowym wyprzedzeniem. Sprzęt będzie dostarczony przez Wykonawcę osobiście lub za pośrednictwem firmy kurierskiej. W przypadku korzystania z pośrednictwa firmy kurierskiej, Wykonawca poda Zamawiającemu jej nazwę oraz numer przesyłki.
3. Wykonawca ponosi koszty ubezpieczenia i transportu sprzętu do siedziby Zamawiającego.
4. Wykonawca udziela Zamawiającemu ……. miesięcznej gwarancji, rozpoczynającej swój bieg od daty podpisania protokołu odbioru;
5. Zamawiający może korzystać uprawnień z tytułu rękojmi za wady sprzętu niezależnie od uprawnień wynikających z gwarancji.
6. W ramach udzielonej gwarancji Wykonawca zobowiązuje się do bezpłatnego usunięcia wad sprzętu w terminie 14 dni od dnia zgłoszenia reklamacji sprzętu.
7. W przypadku nie wykonywania obowiązków gwarancyjnych Zamawiający uprawniony jest do zlecenia naprawy lub usunięcia wady osobie trzeciej na koszt Wykonawcy.

§3
WYNAGRODZENIE I WARUNKI PŁATNOŚCI

1. Wynagrodzenie Wykonawcy za zrealizowanie całej umowy wynosi
   netto …… zł
   VAT 23 % tj. ……zł,
   brutto: ……..zł
   (słownie: …….).

2. Zapłata wynagrodzenia Wykonawcy nastąpi przelewem na następujący rachunek Wykonawcy …….. w ciągu w ciągu 30 dni od dnia otrzymania przez Zamawiającego prawidłowej i wystawionej zgodnie z umową faktury VAT. Data wystawienia faktury nie może być wcześniejsza niż data dostawy sprzętu. W przypadku gdyby Wykonawca zamieścił na fakturze inny termin płatności niż określony w niniejszej umowie, obowiązuje termin płatności określony w umowie.
3. Za datę płatności uznaje się datę obciążenia rachunku Zamawiającego.

§4
KARY UMOWNE

1. Wykonawca zapłaci Zamawiającemu kary umowne:

a) w wysokości 0,5 % kwoty wynagrodzenia brutto określonego w § 3 ust. 1 umowy - za każdy dzień opóźnienia w zrealizowaniu umowy;
b) w wysokości 0,5 % kwoty wynagrodzenia brutto określonego w § 3 ust. 1 umowy - za każdy dzień opóźnienia w usunięciu wady sprzętu w stosunku do określonego w §2 ust. 6 terminu;
c) w wysokości 10% kwoty wynagrodzenia brutto w zakresie właściwej części określonego w § 3 ust. 1 umowy - w przypadku odstąpienia od umowy lub rozwiązania umowy ze skutkiem natychmiastowym z przyczyn, za które odpowiada Wykonawca.

2. Zamawiający ma prawo dochodzenia na zasadach ogólnych odszkodowania uzupełniającego przewyższającego wysokość zastrzeżonych kar umownych.
3. Zamawiający ma prawo dochodzić kar umownych poprzez potrącenie ich na podstawie księgowej noty obciążeniowej z jakimikolwiek należnościami Wykonawcy, aż do całkowitego zaspokojenia roszczeń. W przypadku braku możliwości zaspokojenia roszczeń z tytułu kar umownych na zasadach określonych powyżej, księgowa nota obciążeniowa płatna będzie do 14 dni od daty jej wystawienia przez Zamawiającego.

§5
ROZWIĄZANIE I ODSTĄPIENIE OD UMOWY

1. Zamawiający może odstąpić od umowy, jeśli Wykonawca opóźnia się z realizacją umowy przez co najmniej 2 tygodnie względem terminu określonego w § 2 ust. l umowy.
2. W razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o tych okolicznościach. W takim wypadku Wykonawca może żądać jedynie wynagrodzenia należnego mu z tytułu wykonania części umowy.

§6
POSTANOWIENIA KOŃCOWE

1. W sprawach niniejszą umową nieuregulowanych mają zastosowanie odpowiednie przepisy Kodeksu cywilnego.
2. Jeśli polubowne rozwiązanie sporu nie będzie możliwe spór zostanie rozstrzygnięty przez właściwy sąd powszechny w Katowicach.
3. Wykonawca nie może bez uzyskania wcześniejszej pisemnej zgody Zamawiającego, przelać jakichkolwiek praw lub obowiązków wynikających z niniejszej umowy na osoby trzecie. Czynność prawna mająca na celu

zmianę wierzyciela może nastąpić wyłącznie po uprzednim wyrażeniu pisemnej zgody przez podmiot tworzący Zamawiającego.

4. Wszelkie zmiany treści umowy wymagają zgody obu stron wyrażonej na piśmie pod rygorem nieważności.
5. Umowę sporządzono w 3 egzemplarzach, w tym 1 dla Wykonawcy, a 2 dla Zamawiającego.

Załącznik do umowy:

1) Formularz asortymentowo-cenowy
2) Zestawienie Parametrów Technicznych

Wykonawca **Zamawiający**