PCMG/P-36/2017

Grójec dnia 21.06.2018r.

**SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA**

**Po zmianach w dniu 21 czerwca 2018 roku**

*na zakup, instalację, uruchomienie urządzeń teleinformatycznych i oprogramowania w zakresie objętym projektem pn. „Poprawa jakości i dostępności świadczeń zdrowotnych dzięki wdrożeniu e-usług w Powiatowym Centrum Medycznym w Grójcu”*

Wartość szacunkowa zamówienia nie przekracza równowartości kwoty

221 000 Euro

*Sporządził: Hubert Wasila*

PCMG/P-36/2017

**KARTA UZGODNIEŃ**

do postępowania nr PCMG/P-36/2017

*na zakup, instalację, uruchomienie urządzeń teleinformatycznych i oprogramowania wraz kompleksowym wdrożeniem w zakresie objętym projektem pn. „Poprawa jakości i dostępności świadczeń zdrowotnych dzięki wdrożeniu e-usług w Powiatowym Centrum Medycznym w Grójcu”*

Grójec, dnia 21.06.2018r.

Sporządzający SIWZ: Hubert Wasila

Uzgadniam pod względem wymaganego
zakresu zamówienia i warunków jego realizacji — Włodzimierz Bednarski
(Dyrektor ds. Eksploatacyjno-Administracyjnych )

Uzgadniam i potwierdzam zabezpieczenie
środków finansowych — Beata Wiewiór
(Główny Księgowy)

Potwierdzam, że treść SIWZ jest zgodna
pod względem formalno-prawnym — Karolina Wojtczak
(Radca Prawny)

Potwierdzam, że warunki postępowania zostały
uzgodnione i zaakceptowane przez Komisję Przetargową
i są zgodne z ustawą Prawo zamówień publicznych — Paweł Radwański
(Przewodniczący Komisji Przetargowej)

Grójec, dnia 21.06.2018r.

Zatwierdzam przedłożone dokumenty i wyrażam zgodę na rozpoczęcie postępowania

Marzena Barwicka
(Prezes Powiatowego Centrum Medycznego w Grójcu Sp. z o.o.)

***ROZDZIAŁ I.***

***INSTRUKCJA DLA WYKONAWCÓW***

***ROZDZIAŁ II.***

***OPIS PRZEDMIOTU ZAMÓWIENIA***

***ROZDZIAŁ III. UMOWA (wzór)***

***FORMULARZ OFERTY I FORMULARZE ZAŁĄCZNIKÓW***

***Załącznik nr 1 do formularza oferty***

*OŚWIADCZENIE*

***Załącznik nr 2 do formularza oferty***

*OŚWIADCZENIE*

***Załącznik nr 3 do formularza oferty***

*Wzór oświadczenia wymaganego od wykonawcy w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO*

***Załącznik nr 2 do SIWZ***

*Oświadczenie o przynależności / braku przynależności do grupy kapitałowej*

***Załącznik nr 3 do umowy***

*PROTOKÓŁ DOSTAWY, MONTAŻU, PIERWSZEGO URUCHOMIENIA, SZKOLENIA PERSONELU I ODBIORU, ODBIORU PRZEDMIOTU ZAMÓWIENIA*

***ROZDZIAŁ I.***

***INSTRUKCJA DLA WYKONAWCÓW***

## 1. *ZAMAWIAJĄCY*

| | |
|---|---|
| Zamawiającym jest: | **Powiatowe Centrum Medyczne w Grójcu** |
| | **Spółka z ograniczoną odpowiedzialnością** |
| Adres: | **ul. Ks. Piotra Skargi 10, 05-600 Grójec** |
| Tel.: | **+48 48 664 91 01** |
| Fax: | **+48 48 664 21 81** |
| E-mail: | zamowienia@pcmg.pl |
| Adres strony internetowej: | www.pcmg.pl |
| NIP: | 797-201-92-61 |
| Nazwa banku i nr konta: | PKO BP 61 1020 1042 0000 8302 0363 3443 |

## 2. *OPIS SPOSOBU POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI WRAZ ZE WSKAZANIEM PRZEZ ZAMAWIAJĄCEGO OSÓB UPRAWNIONYCH DO KONTAKTÓW*

**2.1.** Wszelkiego rodzaju oświadczenia, wnioski, zawiadomienia oraz informacje itp. Zamawiający i Wykonawcy przekazują pisemnie, faksem lub pocztą elektroniczną. Oferty, oświadczenia, umowy oraz dokumenty wymienione w pkt. 7 niniejszej instrukcji Wykonawcy przekazują wyłącznie w formie pisemnej.

**2.2.** Jeżeli Zamawiający i Wykonawca przekazują oświadczenia, wnioski, zawiadomienia oraz informacje przekazane za pomocą faksu lub drogą elektroniczną, każda ze stron na żądanie drugiej niezwłocznie potwierdza fakt ich otrzymania.

**2.3.** Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na adres:

**Powiatowe Centrum Medyczne w Grójcu Sp. z o.o.**
**05-600 Grójec, ul. Ks. Piotra Skargi 10**
**Budynek „DOMONT" I piętro Zarząd PCMG**
**Fax 48 664 21 81**
**zamowienia@pcmg.pl**

**2.4.** Osobami uprawnionymi do kontaktów z Wykonawcami są:

**Hubert Wasila – tel. 48 664 91 08**

## 3. TRYB UDZIELENIA ZAMÓWIENIA:

**3.1.** Postępowanie o udzielenie zamówienia prowadzone jest w trybie **przetargu nieograniczonego poniżej 221.000 Euro** na podstawie **art. 39** ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (Dz. U. z 2015r. poz. 2164 ze zm.).

**3.2.** Ilekroć w niniejszej Instrukcji Dla Wykonawców użyte jest pojęcie **„Ustawa Pzp"**, należy przez to rozumieć ustawę Prawo zamówień publicznych, o której mowa w pkt. 3.1.

**4. OPIS PRZEDMIOTU ZAMÓWIENIA**

**4.1. Przedmiotem zamówienia jest zakup, instalacja, uruchomienie urządzeń teleinformatycznych i oprogramowania w zakresie objętym projektem pn. „Poprawa jakości i dostępności świadczeń zdrowotnych dzięki wdrożeniu e-usług w Powiatowym Centrum Medycznym w Grójcu"**

Procedura realizowana jest w ramach projektu "Poprawa jakości i dostępności świadczeń zdrowotnych dzięki wdrożeniu usług e-zdrowia w Powiatowym Centrum Medycznym w Grójcu Sp. z o. o." dofinansowanego z Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020, nr Umowy o dofinansowanie RPMA.02.01.01-14-2486/15-00

**4.2.** Przedmiot zamówienia nazywany jest w dalszej treści niniejszej Instrukcji dla Wykonawców „**Przedmiotem zamówienia**".

**4.3. CPV :**

- CPV: 48000000-8- Pakiety oprogramowania i systemy informatyczne,
- CPV: 48620000-0- Systemy operacyjne,
- CPV: 32420000-3- Urządzenia sieciowe,
- CPV: 30213000-5- Komputery osobiste
- CPV: 30231000-7- Ekrany i konsole komputerowe
- CPV: 30213100-6- Komputery przenośne
- CPV: 48900000-7- Różne pakiety oprogramowania i systemy komputerowe
- CPV: 72265000-0- Usługi konfiguracji oprogramowania
- CPV: 72268000-1- Usługi dostawy oprogramowania
- CPV: 72000000-5- Usługi informatyczne
- CPV: 79632000-3- Szkolenie pracowników
- CPV: 80533100-0- Usługi szkolenia komputerowego

**4.4**.Szczegółowo przedmiot zamówienia określony został w Opisie przedmiotu zamówienia w Rozdziale II SIWZ

***5.* TERMIN WYKONANIA PRZEDMIOTU ZAMÓWIENIA:**

**Termin wykonania zamówienia: 4 tygodnie od daty zawarcia umowy**

## 6. WARUNKI UDZIAŁU W POSTĘPOWANIU

**6.1. o udzielenie zamówienia mogą ubiegać się Wykonawcy którzy:**

**6.1.1.** Nie podlegają wykluczeniu;

**6.1.2.** Spełniają warunki udziału w postępowaniu w zakresie:

**6.1.2.a.** kompetencje lub uprawnienia do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów - zamawiający nie uszczegóławia tego warunku.

**6.1.2.b.** sytuacji ekonomicznej lub finansowej - Zamawiający nie określa szczegółowego warunku w tym zakresie.

**6.1.2.c.** zdolności technicznej lub zawodowej – Zamawiający nie określa szczegółowego warunku w tym zakresie.

**6.1.3.** Zamawiający może na każdym etapie postępowania, uznać, że Wykonawca nie posiada wymaganych zdolności, jeżeli zaangażowanie zasobów technicznych lub zawodowych Wykonawcy w inne przedsięwzięcia gospodarcze Wykonawcy, może mieć negatywny wpływ na realizację zamówienia.

**6.1.4. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia:**

**6.1.4.a.** Jeżeli wykonawcy ubiegają się wspólnie o udzielenie zamówienia, to ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego;

**6.1.4.b.** Przepisy dotyczące Wykonawcy stosuje się odpowiednio do Wykonawców wspólnie ubiegających się o udzielenie zamówienia;

**6.1.4.c.** Jeżeli oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia, została wybrana Zamawiający może żądać przed zawarciem umowy w sprawie zamówienia publicznego umowy regulującej współpracę tych Wykonawców;

**6.1.4.d.** Przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Zamawiający rozumie również Wykonawców będących wspólnikami spółki cywilnej.

**6.1.5.** Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych, lub sytuacji

finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.

**6.1.5.a** Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.

**6.1.5.b** Zamawiający ocenia, czy udostępniane Wykonawcy przez inne podmioty zdolności techniczne lub zawodowe, lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu oraz bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, o których mowa w art. 24 ust. 1 pkt 13–22 i ust. 5 ustawy Pzp.

**6.1.5.c** Wykonawca, który polega na sytuacji finansowej lub ekonomicznej innych podmiotów, odpowiada solidarnie z podmiotem, który zobowiązał się do udostępnienia zasobów, za szkodę poniesioną przez Zamawiającego powstałą wskutek nieudostępnienia tych zasobów, chyba że za nieudostępnienie zasobów nie ponosi winy.

**6.1.5.d** Jeżeli zdolności techniczne lub zawodowe lub sytuacja ekonomiczna lub finansowa, podmiotu, o którym mowa w pkt.6.1.4, nie potwierdzają spełnienia przez Wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tych podmiotów podstawy wykluczenia, Zamawiający żąda, aby Wykonawca w terminie określonym przez Zamawiającego:

1) zastąpił ten podmiot innym podmiotem lub podmiotami lub

2) zobowiązał się do osobistego wykonania odpowiedniej części zamówienia, jeżeli wykaże zdolności techniczne lub zawodowe lub sytuację finansową lub ekonomiczną, o których mowa w pkt.6.1.2.c i 6.1.2.b

## 6.A PODSTAWY WYKLUCZENIA O KTÓRYCH MOWA W ART.24 UST.5 USTAWY PZP.

**6.A.1.** Z postępowania o udzielenie zamówienia Zamawiający wykluczy Wykonawcę:

1) w stosunku do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez

likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (Dz. U. z 2015 r. poz. 978, 1259, 1513, 1830 i 1844 oraz z 2016 r. poz. 615) lub którego upadłość ogłoszono, z wyjątkiem Wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację jego majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (Dz. U. z 2015 r. poz. 233, 978, 1166, 1259 i 1844 oraz z 2016 r. poz. 615);

2) który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy Wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co Zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych;

3) jeżeli wykonawca lub osoby, o których mowa w art. 24 ust. 1 pkt 14 ustawy Pzp, uprawnione do reprezentowania Wykonawcy pozostają w relacjach określonych w art. 17 ust. 1 pkt 2–4 ustawy Pzp z:

a) Zamawiającym,

b) osobami uprawnionymi do reprezentowania Zamawiającego,

c) członkami komisji przetargowej,

d) osobami, które złożyły oświadczenie, o którym mowa w art. 17 ust. 2a ustawy Pzp – chyba że jest możliwe zapewnienie bezstronności po stronie Zamawiającego w inny sposób niż przez wykluczenie Wykonawcy z udziału w postępowaniu;

4) który, z przyczyn leżących po jego stronie, nie wykonał albo nienależycie wykonał w istotnym stopniu wcześniejszą umowę w sprawie zamówienia publicznego lub umowę koncesji, zawartą z Zamawiającym, o którym mowa w art. 3 ust. 1 pkt 1–4 ustawy Pzp, co doprowadziło do rozwiązania umowy lub zasądzenia odszkodowania;

5) będącego osobą fizyczną, którego prawomocnie skazano za wykroczenie przeciwko prawom pracownika lub wykroczenie przeciwko środowisku, jeżeli za jego popełnienie wymierzono karę aresztu, ograniczenia wolności lub karę grzywny nie niższą niż 3000 złotych;

6) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za wykroczenie, o którym mowa w pkt 5;

7) wobec którego wydano ostateczną decyzję administracyjną o naruszeniu obowiązków wynikających z przepisów prawa pracy, prawa ochrony środowiska lub przepisów o zabezpieczeniu społecznym, jeżeli wymierzono tą decyzją karę pieniężną nie niższą niż 3000 złotych;

8) który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych, z wyjątkiem przypadku, o którym mowa w art. 24 ust. 1 pkt 15 ustawy Pzp, chyba że Wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności.

**6.A.2. Procedura odwrócona. Zamawiający nie będzie stosował procedury odwróconej.**

***7.* WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW, POTWIERDZAJĄCYCH SPEŁNIENIE WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ BRAK PODSTAW WYKLUCZENIA:**

**7.1.** W niniejszym postępowaniu o udzielenie zamówienia Zamawiający żąda od Wykonawców wyłącznie oświadczeń lub dokumentów niezbędnych do przeprowadzenia postępowania, t.j. oświadczeń lub dokumentów potwierdzających:

1) spełnianie warunków udziału w postępowaniu lub kryteria selekcji,

2) spełnianie przez oferowane dostawy, usługi lub roboty budowlane wymagań określonych przez Zamawiającego,

3) brak podstaw wykluczenia.

**7.2 Do oferty każdy Wykonawca zobowiązany jest załączyć:**

**7.2.1)** aktualne na dzień składania ofert oświadczenie Wykonawcy składane na podstawie art. 25a ust.1 ustawy Pzp – dotyczące spełnienia warunków udziału w postępowaniu – według wzoru stanowiącego załącznik nr 1 do FORMULARZA OFERTY /treść informacji zawartych w niniejszym oświadczeniu stanowić będzie potwierdzenie, że Wykonawca nie

podlega wykluczeniu z postępowania oraz spełnia warunki udziału w niniejszym postępowaniu./

**7.2.2)** Na potwierdzenie, że oferowane dostawy odpowiadają wymaganiom określonym przez Zamawiającego należy załączyć do oferty **poprawnie wypełnioną specyfikację techniczną dla oferowanej części.**

**7.2.3)** Pełnomocnictwo do reprezentowania Wykonawcy /dokument złożony w oryginale lub notarialnie poświadczona jego kopia - jeżeli dotyczy/

**7.3.** W przypadku kiedy o zamówienie ubiegają się Wykonawcy wspólnie, oświadczenie składane na podstawie art.25a ust.1 ustawy Pzp – dotyczące spełnienia warunków udziału w postępowaniu – według wzoru stanowiącego załącznik nr 1 do Formularza oferty - składa każdy z Wykonawców wspólnie ubiegających się o zamówienie.

**7.4.** Wykonawca, który zamierza powierzyć wykonanie części zamówienia podwykonawcom, w celu wykazania braku istnienia wobec nich podstaw wykluczenia z udziału w postępowaniu: zamieszcza informacje o podwykonawcach w oświadczeniu, o którym mowa w ust. 7.2.1.).

**7.5.** Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełniania, w zakresie, w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu lub kryteriów selekcji: zamieszcza informacje o tych podmiotach w oświadczeniu, o którym mowa w ust. 7.2.1.).

**7.6. Wykonawca wraz z oferta zobowiązany jest do złożenia aktualnych na dzień składania ofert oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy Pzp tj.:**

**7.6.1)** wykaz oświadczeń i dokumentów, składanych przez Wykonawców w niniejszym postępowaniu na wezwanie Zamawiającego w celu potwierdzenia okoliczności, o których mowa w art. 25 ust.1 pkt 3 ustawy Pzp: **odpis z właściwego rejestru lub Centralnej Ewidencji i Informacji o Działalności Gospodarczej - jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw do wykluczenia na podstawie art.24 ust.5 pkt 1 ustawy Pzp.**

**7.6.2)** wykaz oświadczeń i dokumentów, składanych przez Wykonawców w niniejszym postępowaniu w celu potwierdzenia okoliczności, o których mowa w art.25 ust.1 pkt 1 ustawy Pzp:

**7.6.3)** wykaz oświadczeń i dokumentów, składanych przez Wykonawców w niniejszym postępowaniu w celu potwierdzenia okoliczności, o których mowa w art. 25 ust. 1 pkt 2 ustawy Pzp:

**7.6.4. oświadczenie wymagane od wykonawcy w zakresie wypełniania obowiązków informacyjnych przewidzianych w art.13 lub art.14 RODO- złącznik nr 1**

**7.7**. Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art.24 ust. 1 pkt 23 ustawy Pzp. Wraz z tym oświadczeniem Wykonawca może złożyć dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w niniejszym postępowaniu o udzielenie zamówienia publicznego – **oświadczenie to musi zostać złożone w terminie 3 dni od dnia zamieszczenia przez Zamawiającego na stronie internetowej informacji, o której mowa w art. 86 ust.5 ustawy Pzp.**

**7.8.** Jeżeli Wykonawca nie złożył oświadczenia, o którym mowa w pkt.7.2.1, oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy Pzp, lub innych dokumentów niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez Zamawiającego wątpliwości, Zamawiający wzywa do ich złożenia, uzupełnienia lub poprawienia lub do udzielania wyjaśnień w terminie przez siebie wskazanym, chyba że mimo ich złożenia, uzupełnienia lub poprawienia lub udzielenia wyjaśnień oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.

**7.9.** Jeżeli Wykonawca nie złożył wymaganych pełnomocnictw albo złożył wadliwe pełnomocnictwa, Zamawiający wzywa do ich złożenia w terminie przez siebie wskazanym, chyba że mimo ich złożenia oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.

**7.10**. Zamawiający wzywa także, w wyznaczonym przez siebie terminie, do złożenia wyjaśnień dotyczących oświadczeń lub dokumentów, o których mowa w art. 25 ust.1 ustawy Pzp.

**7.11. PODWYKONAWCY:** zgodnie z art. 36a ust.1 ustawy Pzp Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy, Zamawiający żąda, aby Wykonawca wskazał w

swojej ofercie części zamówienia, które zamierza powierzyć do wykonania przez podwykonawcę i podania przez Wykonawcę firm podwykonawców / wskazać w formularzu oferty w pkt.8/

**7.12.** w zakresie nieuregulowanym niniejszą instrukcją zastosowanie mają przepisy Rozporządzenia Ministra Rozwoju z dnia 26 lipca 2016r. w sprawie rodzajów dokumentów, jakich można żądać od wykonawcy w postępowaniu o udzielenie zamówienia (Dz.U. 2016 poz. 1126).

**8. WADIUM**

**8.1.** Warunkiem udziału w postępowaniu jest wniesienie Wadium.

**8.2.** Zamawiający określa wadium w wysokości:

**3 600,00 zł /**słownie: trzy tysiące sześćset złotych/,

***8.3.*** Wadium musi być wniesione do dnia **2018.06.25 do godz**. **13:00.**

**8.4** Wadium można wnieść w następujących formach, w:

**8.4.1** pieniądzu, przelewem na rachunek bankowy Zamawiającego:

PKO Bank Polski S.A. **61 1020 1042 0000 8302 0363 3443**

**8.4.2** poręczeniach bankowych,

**8.4.3** gwarancjach bankowych,

**8.4.4**.gwarancjach ubezpieczeniowych,

**8.4.5** poręczeniach udzielanych przez podmioty, o których mowa w art. 6 ust. 3 pkt. 4 lit. b ustawy z dnia 9 listopada 2000 r. o Utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. Nr 109 poz. 1158 z póź. zm).

Jeżeli wadium zostanie wniesione w pieniądzu, przelewem Wykonawca dołącza do oferty kserokopię wpłaty wadium z potwierdzeniem dokonanego przelewu. Na poleceniu przelewu należy wpisać „Wadium - przetarg nieograniczony poniżej 221.000 Euro na **zakup, instalacja, uruchomienie urządzeń teleinformatycznych i oprogramowania w zakresie objętym projektem pn. „Poprawa jakości i dostępności świadczeń zdrowotnych dzięki wdrożeniu e-usług w Powiatowym Centrum Medycznym w Grójcu”.**

**8.5.** W przypadku wniesienia wadium w formie pieniężnej o jego wniesieniu w termie decydować będzie data wpływu środków na rachunek bankowy Zamawiającego.

**8.6.** W przypadku wniesienia wadium w formie o której mowa w pkt. 8.4.2- 8.4.5 wymagane jest dołączenie do oferty oryginału dokumentu wystawionego na rzecz Zamawiającego.

Dokumenty te muszą być ważne przez cały okres związania Wykonawcy złożoną przez niego ofertą.

**8.7.** Okoliczności i zasady zwrotu wadium określone są w ustawie Prawo zamówień publicznych art. 46 ustawy pzp.

**9. OPIS SPOSOBU PRZYGOTOWANIA OFERT:**

**9.1.** Wykonawca może złożyć tylko jedną ofertę.

**9.2.** Zamawiający **nie dopuszcza** możliwości składania ofert częściowych.

**9.3**. Zamawiający nie dopuszcza możliwości składania ofert wariantowych.

**9.4**. Zamawiający nie przewiduje udzielenia zamówień **na dodatkowe dostawy** na podstawie art. 67 ust. 1 pkt. 7 ustawy Pzp.

**9.5.** Oferta musi być sporządzona z zachowaniem formy pisemnej pod rygorem nieważności.

**9.6.** Każdy dokument składający się na ofertę musi być czytelny.

**9.7.** Oferta musi być podpisana przez Wykonawcę. Zamawiający wymaga, aby ofertę podpisano zgodnie z zasadami reprezentacji wskazanymi we właściwym rejestrze lub ewidencji działalności gospodarczej. Jeżeli osoba/osoby podpisująca ofertę działa na podstawie pełnomocnictwa, to pełnomocnictwo to musi w swej treści jednoznacznie wskazywać uprawnienie do podpisania oferty. Pełnomocnictwo to musi zostać dołączone do oferty i musi być złożone w oryginale lub kopii poświadczonej notarialnie.

**9.8.** Oferta musi być sporządzona w języku polskim. Każdy dokument składający się na ofertę sporządzony w innym języku niż język polski winien być złożony wraz z tłumaczeniem na język polski. W razie wątpliwości uznaje się, iż wersja polskojęzyczna jest wersją wiążącą.

**9.9.** Dokumenty składające się na ofertę mogą być złożone w oryginale lub kserokopii potwierdzonej za zgodność z oryginałem przez Wykonawcę.

**9.10.** Zaleca się by każda zawierająca jakąkolwiek treść strona była podpisana lub parafowana przez Wykonawcę. Każda poprawka w treści oferty, a w szczególności każde przekreślenie, przerobienie, uzupełnienie, nadpisanie, przesłonięcie korektorem, etc. powinny być parafowane oraz datowane przez Wykonawcę.

**9.11.** Strony oferty winny być trwale ze sobą połączone i kolejno ponumerowane. W treści oferty winna być umieszczona informacja o ilości stron.

**9.12.** W przypadku gdy informacje zawarte w ofercie stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji, co do, których Wykonawca zastrzega, że nie mogą być udostępniane innym uczestnikom postępowania, muszą być oznaczone klauzulą: ”Informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003r. nr 153 poz. 1503).” i dołączone do oferty, zaleca się aby były trwale, oddzielnie spięte.

Zgodnie z art. 8 ust. 3 ustawy Pzp, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, nie później niż w terminie składania ofert o dopuszczenie do udziału w postępowaniu zastrzegł, że nie mogą być one udostępnione oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust. 4 ustawy Pzp. parafowane własnoręcznie przez osobę upoważnioną do reprezentowania Wykonawcy.

**9.13.** Złożenie więcej niż jednej oferty lub złożenie oferty zawierającej propozycje alternatywne powoduje odrzucenie wszystkich ofert złożonych przez Wykonawcę.

**9.14.** Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

**9.15**. Oferta musi obejmować całość zamówienia w zakresie części.

**9.16.** Formularz oferty, inne oświadczenia oraz wykazy, o których mowa w specyfikacji muszą być podpisane przez osobę upoważnioną do reprezentowania Wykonawcy.

## 10. OPIS SPOSOBU UDZIELANIA WYJAŚNIEŃ TREŚCI SIWZ:

**10.1.** Wykonawca może zwrócić się do Zamawiającego z pisemną prośbą o wyjaśnienie treści SIWZ. Zamawiający odpowie na piśmie na zadane pytanie, przesyłając treść pytania i odpowiedzi wszystkim zidentyfikowanym uczestnikom postępowania oraz umieści taką informację na własnej stronie internetowej (www.pcmg.pl), pod warunkiem, że pytanie wpłynie do Zamawiającego, **nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu do składania ofert.**

**10.2. Zamawiający udzieli wyjaśnień, niezwłocznie jednak nie później niż:**

**a) na 2 dni przed upływem terminu składania ofert**

**10.3.** Pytania należy kierować na adres:

**Powiatowe Centrum Medyczne w Grójcu**
**spółka z ograniczoną odpowiedzialnością**
**05-600 Grójec**
**ul. Ks. Piotra Skargi 10**
**Fax: +48 48 664 21 81**
**Email: zamowienia@pcmg.pl**

**10.4.** W przypadku rozbieżności pomiędzy treścią niniejszej SIWZ a treścią udzielonych odpowiedzi, jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.

**10.5.** Zamawiający nie przewiduje zwołania zebrania wszystkich Wykonawców w celu wyjaśnienia treści SIWZ.

**10.6.** W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść SIWZ. Dokonaną zmianę SIWZ Zamawiający udostępnia na stronie internetowej.

**10.7.** Jeżeli zmiana SIWZ będzie prowadziła do zmiany treści ogłoszenia o zamówieniu, Zamawiający zamieści zmienione ogłoszenie w Biuletynie Zamówień Publicznych.

**10.8.** Zamawiający przedłuży termin składania ofert, jeżeli w wyniku zmiany treści SIWZ **nie prowadzącej do zmiany treści ogłoszenia** o zamówieniu**,** jest niezbędny dodatkowy czas na wprowadzanie zmian w ofertach i poinformuje o tym Wykonawców, którym przekazano SIWZ oraz na stronie internetowej: (www.pcmg.pl).

**10.9. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku z zapytaniem, o którym mowa w pkt.10.1**

## 11. OPIS SPOSOBU OBLICZENIA CENY OFERTY:

**11.1.** Cena oferty powinna zostać wyliczona przez Wykonawcę i przedstawiona w składanej ofercie. Cena oferty winna być podana w złotych polskich liczbowo i słownie. Zamawiający nie dopuszcza rozliczeń między stronami w walutach obcych.

**11.2.** Każdy z Wykonawców może zaproponować tylko jedną cenę i nie może jej zmienić.

**11.3.** Wykonawca uwzględniając wszystkie wymogi, o których mowa w niniejszej Specyfikacji Istotnych Warunków Zamówienia, powinien w cenie ofertowej ująć wszelkie koszty związane z wykonaniem przedmiotu zamówienia, niezbędne dla prawidłowego i pełnego wykonania przedmiotu zamówienia. W cenie oferty należy uwzględnić podatek od towarów i usług oraz podatek akcyzowy, jeżeli na podstawie odrębnych przepisów sprzedaż towarów podlega

obciążeniu podatkiem od towarów i usług lub podatkiem akcyzowym z uwzględnieniem postanowień pkt.11.4.

**11.4.** Jeżeli Zamawiającemu zostanie złożona oferta, której wybór prowadziłby do powstania obowiązku podatkowego Zamawiającego zgodnie z przepisami o podatku od towarów i usług Zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek wpłacić zgodnie z obowiązującymi przepisami.

Wykonawca składając ofertę informuje Zamawiającego, czy wybór oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania oraz wskazuje ich wartość bez kwoty podatku /należy wskazać w formularzu oferty pkt.11/

**11.5.** Stawkę podatku vat należy określić zgodnie z ustawą z dnia 11 marca 2004r. o podatku od towarów i usług (tekst jednolity Dz.U. z 2011r. nr 11 poz.1054 ze zm.).

## 12. MIEJSCE I TERMIN SKŁADANIA OFERT

**12.1.** Ofertę należy złożyć w siedzibie Powiatowego Centrum Medycznego w Grójcu spółka z ograniczoną odpowiedzialnością z siedzibą w Grójcu przy ul. Ks. Piotra Skargi 10 w sekretariacie Budynek D, osobiście lub za pośrednictwem operatora pocztowego **w terminie do 2018.06.25 do godziny 13.00**

**12.2.** Ofertę należy umieścić w zamkniętym opakowaniu, uniemożliwiającym odczytanie zawartości bez uszkodzenia tego opakowania. Opakowanie powinno być oznaczone nazwą (firmą) i adresem Wykonawcy, zaadresowane na adres Powiatowe Centrum Medyczne w Grójcu spółka z ograniczoną odpowiedzialnością – SEKRETARIAT - 05-600 Grójec, ul. Ks. Piotra Skargi 10 oraz opisane **„Oferta przetargowa na zakup, instalację, uruchomienie urządzeń teleinformatycznych i oprogramowania w zakresie objętym projektem pn. „Poprawa jakości i dostępności świadczeń zdrowotnych dzięki wdrożeniu e-usług w Powiatowym Centrum Medycznym w Grójcu”. Nie otwierać przed dniem 2018.06.25. do godz.13.30”**

**12.3.** W niniejszym postępowaniu Zamawiający zgodnie z art. 84 ust. 2 ustawy Pzp niezwłocznie zwraca ofertę, która została złożona po terminie.

**12.4.** Wykonawca może wprowadzić zmiany, poprawki, modyfikacje i uzupełnienia, do złożonej oferty, pod warunkiem, że Zamawiający otrzyma pisemne zawiadomienie o wprowadzeniu

zmian przed terminem składania ofert. Powiadomienie o wprowadzeniu zmian musi być złożone według takich samych zasad, jak składana oferta, tj. w kopercie odpowiednio oznakowanej napisem „ZMIANA" i z powołaniem się na numer, pod jakim została zarejestrowana oferta. Koperty oznaczone „ZMIANA" zostaną otwarte przy otwieraniu oferty Wykonawcy, który wprowadził zmiany i po stwierdzeniu poprawności procedury dokonywania zmian, zostaną dołączone do oferty.

**12.5.** Wykonawca ma prawo przed upływem terminu składania ofert zmienić lub wycofać ofertę poprzez złożenie pisemnego powiadomienia podpisanego przez osobę upoważnioną do reprezentowania Wykonawcy.

***13. TERMIN ZWIĄZANIA OFERTĄ***

**13.1.** Termin związania ofertą wynosi **30 dni.** Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

**13.2.** Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą, z tym że Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofert, zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.

***14. MIEJSCE I TERMIN OTWARCIA OFERT***

**14.1.** Otwarcie ofert nastąpi w siedzibie Powiatowego Centrum Medycznego w Grójcu spółka z ograniczoną odpowiedzialnością z siedziba w Grójcu przy ul. Ks. Piotra Skargi 10 **, w pok. nr 21 /Sala Konferencyjna/, w dniu 2018.06.25, godz. 13.30**

**14.2.** Otwarcie ofert jest jawne.

**14.3.** Bezpośrednio przed otwarciem ofert Zamawiający poda kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia.

**14.4.** Podczas otwarcia ofert zostaną podane: nazwy (firmy) oraz adresy Wykonawców, a także informacje dotyczące ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

**14.5.** Niezwłocznie po otwarciu ofert Zamawiający zamieści na stronie internetowej www.pcmg.pl informacje dotyczące:

**14.5.1.** kwoty, jaka zamierza przeznaczyć na sfinansowanie zamówienia,

**14.5.2.** firm oraz adresów Wykonawców, którzy złożyli oferty w terminie,

**14.5.3.** ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

***15. OPIS KRYTERIÓW KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW***

**15.1.** Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami i ich znaczeniem:

Cena – 60 % / maksymalna ilość punktów jaka może otrzymać oferta za dane kryterium - 60/

Okres gwarancji i rękojmi – 40 % / maksymalna ilość punktów jaka może otrzymać oferta za dane kryterium - 40/

**15.2.** Oferta spełniająca w najwyższym stopniu wymagania kryteriów otrzyma maksymalną ilość punktów. Pozostałym Wykonawcom przypisana zostanie proporcjonalnie **odpowiednio mniejsza ilość punktów.**

**15. 3. SPOSÓB OCENY OFERT.**

**15.3..1.** Ocena ofert w zakresie przedstawionych kryteriów zostanie dokonana według następującej zasady:

**a/ Kryterium Cena:**

Wartość punktowa= C min/ C of x R

R- Ranga ocenianego kryterium

C min- najniższa wartość brutto z wszystkich złożonych ofert

C of- wartość brutto oferty badanej

Do oceny ofert w kryterium „cena" będzie brana pod uwagę cena oferty brutto (w zł)

W zakresie kryterium „cena" oferta może uzyskać 95 punktów.

**b/ Kryterium Okres gwarancji i rękojmi**

Wartość punktowa dla kryterium „ Okres gwarancji i rękojmi" będzie wyliczana według wzoru:

Wartość punktowa= T of / Tmax x R

T of – liczba punktów przyznanych ofercie badanej

T max – najwyższy oferowany termin gwarancji

R- Ranga ocenianego kryterium

W zakresie kryterium „ termin gwarancji” oferta może uzyskać 5 punktów.

**UWAGA: Do oceny ofert w kryterium „Okres gwarancji i rękojmi” będzie brana pod uwagę wartość podana w pkt. 4 formularza oferty, wyrażona liczbowo (ilość miesięcy).**

minimalny termin gwarancji wynosi 60 miesięcy.

W przypadku gdy Wykonawca nie wypełni precyzyjnie oferowanego termin gwarancji , Zamawiający do oceny ofert przyjmie najkrótszy termin gwarancji i przyzna 0 pkt.

**15.4.** Obliczenia będą dokonywane z dokładnością do dwóch miejsc po przecinku.

**15.5.** Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny lub kosztu i innych kryteriów oceny ofert, Zamawiający spośród tych ofert wybiera ofertę z najniższą ceną lub najniższym kosztem, a jeżeli zostały złożone oferty o takiej samej cenie lub koszcie, Zamawiający wzywa Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych**.**

**15.6.** Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami.

**15.7.** Za najkorzystniejszą zostanie uznana oferta, która nie podlega odrzuceniu oraz uzyska największą ilość punktów w w/w kryteriach oceny ofert.

## 16. INFORMACJE O FORMALNOŚCIACH JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO:

**16.1.** Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w ustawie Pzp oraz niniejszej specyfikacji i została oceniona jako najkorzystniejsza w oparciu o podane w ogłoszeniu o zamówieniu i SIWZ kryteria wyboru.

**16.2.** W przypadku wyboru za najkorzystniejszą, oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, Zamawiający żąda przed zawarciem umowy, złożenia treści umowy regulującej współpracę tych Wykonawców – jeżeli treść takiej umowy nie została załączona do oferty. Treść tej umowy powinna wyraźnie określać jej strony, cel działania, sposób współdziałania, zakres prac przewidzianych do wykonania każdej stronie umowy, solidarną odpowiedzialność za wykonanie zamówienia, oznaczenie czasu trwania tej umowy w tym obejmującego okres realizacji zamówienia, gwarancji i rękojmi, wykluczenie

możliwości wypowiedzenia tej umowy przez którąkolwiek ze stron / członków konsorcjum/ do czasu wykonania zamówienia.

**16.3.** Umowa o udzielenie zamówienia publicznego w niniejszym postępowaniu zostanie zawarta według wzoru Zamawiającego.

## ***17. ISTOTNE WARUNKI UMOWY***

**17.1.** Przedmiot umowy i jej warunki określone zostały w Rozdziale IV SIWZ – „Wzór umowy".

**17.2.** Zamawiający zawiera umowę w sprawie zamówienia publicznego w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 10 dni – jeżeli zostało przesłane w inny sposób .

**17.3.** Zabezpieczenie należytego wykonania umowy nie jest wymagane.

**17.4.** Wszelkie zmiany do umowy jakie Zamawiający dopuszcza zostały określone we wzorze umowy stanowiącym załącznik do SIWZ.

## ***18. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ***

Odwołanie

**18.1.** Wykonawcy a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy Prawo zamówień publicznych, przysługują środki ochrony prawnej przewidziane w Dziale VI tej ustawy.

**18.2.** Zgodnie z art. 180 ust. 1 i ust.2 ustawy Pzp odwołanie przysługuje wyłącznie wobec czynności:

1) określenia warunków udziału w postępowaniu;
2) wykluczenia odwołującego z postępowania o udzielenie zamówienia;
3) odrzucenia oferty odwołującego;
4) opisu przedmiotu zamówienia;
5) wyboru najkorzystniejszej oferty.

**18.3.** Odwołanie powinno wskazywać czynność lub zaniechanie czynności Zamawiającego, której zarzuca się niezgodność z przepisami ustawy, zawierać zwięzłe przedstawienie zarzutów,

określać żądanie oraz wskazywać okoliczności faktyczne i prawne uzasadniające wniesienie odwołania.

**18.4.** Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej lub w postaci elektronicznej podpisane bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu lub równoważnego środka, spełniającego wymagania dla tego rodzaju podpisu.

**18.5.** Odwołujący przesyła kopię odwołania Zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.

**18.6.** Wykonawca może w terminie przewidzianym do wniesienia odwołania poinformować Zamawiającego o niezgodnej z przepisami ustawy czynności podjętej przez niego lub zaniechaniu czynności, do której jest on zobowiązany na podstawie ustawy, na które nie przysługuje odwołanie na podstawie art. 180 ust.2 ustawy Pzp.

**18.7.** W przypadku uznania zasadności przekazanej informacji Zamawiający powtarza czynność albo dokonuje czynności zaniechanej, informując o tym Wykonawców w sposób przewidziany w ustawie dla tej czynności.

**18.8**. Na czynności, o których mowa w ust. 18.7 nie przysługuje odwołanie z zastrzeżeniem art. 180 ust.2 ustawy Pzp.

**18.9**. Odwołanie wnosi się:

1. w terminie **5 dni** od dnia przesłania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przesłane w sposób określony w art.180 ust.5 zdanie drugie ustawy Pzp albo
2. w terminie **10 dni** – jeżeli zostały przesłane w inny sposób.

**18.10.** Odwołanie wobec treści ogłoszenia o zamówieniu, a jeżeli postępowanie jest prowadzone w trybie przetargu nieograniczonego, także wobec postępowań specyfikacji istotnych warunków zamówienia, wnosi się w terminie:

- **5 dni** od dnia zamieszczenia ogłoszenia w **Biuletynie Zamówień Publicznych** lub specyfikacji istotnych warunków zamówienia na stronie internetowej.

**18.11.** Odwołanie wobec czynności innych niż określone w ust. 18.9 i 18.10 wnosi się:

- w terminie **5 dni** od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia;

**18.12.** W przypadku wniesienia odwołania wobec treści ogłoszenia o zamówieniu lub postanowień specyfikacji istotnych warunków zamówienia Zamawiający może przedłużyć termin składania ofert.

**18.13**. W przypadku wniesienia odwołania po upływie terminu składania ofert bieg terminu związania ofertą ulega zawieszeniu do czasu ogłoszenia przez Krajową Izbę Odwoławczą orzeczenia.

***Skarga do sądu***

**18.14**. Na orzeczenie Krajowej Izby Odwoławczej stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.

**18.15**. Skargę wnosi się do sądu okręgowego właściwego dla siedziby albo miejsca zamieszkania Zamawiającego.

**18.16.** Skargę wnosi się za pośrednictwem Prezesa Urzędu Zamówień Publicznych w terminie 7 dni od dnia doręczenia orzeczenia Krajowej Izby Odwoławczej, przysyłając jednocześnie jej odpis przeciwnikowi skargi.

## 19. POSTANOWIENIA DOTYCZĄCE JAWNOŚCI PROTOKOŁU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA:

**19.1**. Zamawiający udostępnia protokół lub załączniki do protokołu na wniosek.

**19.2.Przekazanie protokołu lub załączników następuje przy użyciu środków komunikacji elektronicznej.**

**19.3. W przypadku protokołu lub załączników sporządzonych w postaci papierowej, jeżeli z przyczyn technicznych znacząco utrudnione jest udostępnienie tych dokumentów przy użyciu środków komunikacji elektronicznej, w szczególności z uwagi na ilość żądanych do udostępnienia dokumentów, Zamawiający informuje o tym Wnioskodawcę i wskazuje sposób, w jaki mogą być one udostępnione.**

**19.4.** Bez zgody Zamawiającego, Wnioskodawca w trakcie wglądu do protokołu lub załączników, w miejscu wyznaczonym przez Zamawiającego, nie może samodzielnie kopiować lub utrwalać za

pomocą urządzeń lub środków technicznych służących do utrwalania obrazu treści złożonych ofert.

**19.5.** Zamawiający udostępnia Wnioskodawcy protokół lub załączniki niezwłocznie. W wyjątkowych przypadkach, w szczególności związanych z zapewnieniem sprawnego toku prac dotyczących badania i oceny ofert, Zamawiający udostępnia odpowiednio oferty w terminie przez siebie wyznaczonym, nie później jednak niż odpowiednio w dniu przekazania informacji o wyborze najkorzystniejszej oferty lub w dniu przekazania informacji o wynikach oceny spełnienia warunków udziału w postępowaniu i otrzymanych ocenach spełniania tych warunków albo w dniu przekazania informacji o unieważnieniu postępowania.

**19.6.** W sprawach nieuregulowanych zastosowanie mają przepisy ustawy Prawo zamówień publicznych.

## 20. KLAUZULA INFORMACYJNA Z ART. 13 RODO DO ZASTOSOWANIA PRZEZ ZAMAWIAJĄCYCH 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 */Powiatowe Centrum Medyczne w Grójcu spółka z ograniczoną odpowiedzialnością z siedzibą w Grójcu przy ul. Piotra Skargi 10 /;*
- inspektorem ochrony danych osobowych w */Powiatowe Centrum Medyczne w Grójcu spółka z ograniczoną odpowiedzialnością /* jest Pani/Pani */Ewelina Średnicka, kontakt: adres sekretariat@pcmg.pl, 48 664-91-01/* *;
  - Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego */ zakup, instalacja, uruchomienie urządzeń teleinformatycznych i oprogramowania w zakresie objętym projektem pn. „Poprawa jakości i dostępności świadczeń zdrowotnych dzięki wdrożeniu e-usług w Powiatowym Centrum Medycznym w Grójcu". P-36 /2018/* prowadzonym w trybie przetargu nieograniczonego;
- 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 2017 r. poz. 1579 i 2018), 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**.

---

* ***Wyjaśnienie:*** *informacja w tym zakresie jest wymagana, jeżeli w odniesieniu do danego administratora lub podmiotu przetwarzającego istnieje obowiązek wyznaczenia inspektora ochrony danych osobowych.*

** ***Wyjaśnienie:*** *skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.*

*** ***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.*

**ROZDZIAŁ II**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest zakup, instalacja, uruchomienie urządzeń teleinformatycznych i oprogramowania w zakresie objętym projektem pn. „Poprawa jakości i dostępności świadczeń zdrowotnych dzięki wdrożeniu e-usług w Powiatowym Centrum Medycznym w Grójcu”

PCMG/P-36/2017

Szczegółowy opis przedmiotu zamówienia:

**Zestawy komputerowe – 10 sztuk**

**Jednostka centralna- 10 sztuk**

| Lp. | Parametr | Charakterystyka (wymagania minimalne) |
|---|---|---|
| 1 | Komputer | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu. |
| 2 | Obudowa | Typu Small Form Factor z obsługą kart PCI Express wyłącznie o niskim profilu.<br>Wyposażona w min. 2 kieszenie: 1 szt. 5,25” zewnętrzna (dopuszcza się w wersji tzw. slim zajętej przez napęd optyczny), 1 szt. 3,5”, możliwość rozbudowy komputera do konfiguracji dwudyskowej w oparciu o dyski w rozmiarach 2.5” + 3,5”.<br>Obudowa musi być wyposażona w czujnik otwarcia obudowy. Obudowa musi mieć możliwość zainstalowania oryginalnego filtra przeciwpyłowego zapobiegającego nadmiernemu gromadzeniu się kurzu w środku obudowy. Filtr musi umożliwiać łatwe czyszczenie bez otwierania obudowy.<br>Wymagana możliwość czyszczenia filtra za pomocą wody. Filtr musi być także opcją producenta komputera możliwą do zamówienia jako część eksploatacyjna. W ofercie należy podać numer katalogowy (PN) części pod jaką można zamówić filtr u producenta komputera.<br>Beznarzędziowe otwieranie obudowy oraz wymiana HDD, ODD i kart rozszerzających.<br>Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem katalogowym PN, numerem seryjnym.<br>Obudowa gotowa do pracy w trybie Pion lub Poziom. |
| 3 | Chipset | Dostosowany do zaoferowanego procesora. |
| 4 | Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji).<br>Wyposażona złącza dla kart PCIe oraz umożliwiająca ich montaż obudowa:<br>1x PCI Express 3.0 x16, 2 x PCI Express 2.0 x1, |
| 5 | Procesor | Procesor osiągający w teście PassMark CPU Mark wynik min. 5900 punktów (wynik zaproponowanego procesora musi znajdować się na stronie: www.cpubenchmark.net). |
| 6 | Pamięć operacyjna | Min. 4 GB RAM, 2400MHz DDR4, 4 sloty na pamięć, z czego 3wolne. Możliwość rozbudowy do 64 GB. |
| 7 | Dysk twardy | Min. 500GB 7200 obr./min., zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |
| 8 | Napęd optyczny | Nagrywarka DVD +/-RW wyposażona w tackę z zaczepami umożliwiającymi pracę w poziomie i pionie. |

| | | |
|---|---|---|
| 9 | Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki.<br>Karta graficzną osiągająca min. 1220 pkt w teście Videocard Benchmark (http://www.videocardbenchmark.net/) |
| 10 | Audio | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. |
| 11 | Karta sieciowa | 10/100/1000 – złącze RJ45 |
| 12 | Porty/złącza | Wbudowane porty: 1 x VGA, 2 x DP, 8 x USB w tym:<br>- z przodu obudowy min.: 4x USB3.1 Gen 1<br>- z tyłu obudowy min.: 2x USB3.1 Gen 1, 2x USB2.0<br>- 1 x port sieciowy RJ-45,<br>- 2 x port szeregowy RS-232<br>- 1 x port równoległy<br>- porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy<br>Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. |
| 13 | Klawiatura/mysz | Klawiatura przewodowa USB w układzie US, wyposażona w czytnik kart mikroprocesorowych; mysz przewodowa USB z rolką (scroll) |
| 14 | Zasilacz | Energooszczędny zasilacz o mocy nie większej niż 210W oraz sprawności na poziomie:<br>• 20% obciążenia 83% sprawności,<br>• na poziomie 50% obciążenia 85% sprawności<br>• na poziomie 100% obciążenia 83% sprawności.<br>Zasilacz musi posiadać certyfikat 80 PLUS klasy min BRONZE. Należy dołączyć certyfikat ze strony https://plugloadsolutions.com/80pluspowersupplies.aspxpotwierdzający spełnianie w/w wymogu. |
| 15 | System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:<br>1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:<br>a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,<br>b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych<br>2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego<br>3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim<br>4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.<br>5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe<br>6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,<br>7. Zlokalizowane w języku polskim, co najmniej następujące elementy: |

| | | |
|---|---|---|
| | | menu, pomoc, komunikaty systemowe, menedżer plików.<br>8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim<br>9. Wbudowany system pomocy w języku polskim.<br>10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).<br>11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.<br>12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.<br>13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.<br>14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.<br>15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.<br>16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".<br>17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.<br>18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.<br>19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.<br>20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.<br>21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.<br>22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.<br>23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."<br>24. Wbudowany mechanizm wirtualizacji typu hypervisor."<br>25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.<br>26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.<br>27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. |

| | | |
|---|---|---|
| | | 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).<br>29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.<br>30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.<br>31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.<br>32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM<br>33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.<br>34. Możliwość tworzenia wirtualnych kart inteligentnych.<br>35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)<br>36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.<br>37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.<br>38. Mechanizmy logowania w oparciu o:<br>a. Login i hasło,<br>b. Karty inteligentne i certyfikaty (smartcard),<br>c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),<br>d. Certyfikat/Klucz i PIN<br>e. Certyfikat/Klucz i uwierzytelnienie biometryczne<br>39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5<br>40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.<br>41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach<br>42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń<br>43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń<br>44. System operacyjny w wersji Proffesional |
| 16 | Oprogramowanie antywirusowe | 1. Pełne wsparcie dla systemu zaproponowanego przez Wykonawcę w ofercie– LICENCJA NA OKRES MINIMUM 60 MIESIĘCY<br>2. Wsparcie dla systemów posiadanych przez Zamawiającego na stanowiskach użytkowników, tzn. MS Windows: XP, Vista, 7, 8, 10<br>3. Wersja programu dla stacji roboczych dostępna zarówno w języku polskim jak i angielskim.<br>**Ochrona antywirusowa i antyspyware**<br>4. Pełna ochrona przed wirusami, trojanami, robakami i innymi |

| | | |
|---|---|---|
| | | zagrożeniami.<br>5. Wbudowana technologia do ochrony przed rootkitami.<br>6. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.<br>7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.<br>8. 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.<br>9. 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<br>10. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.<br>11. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.<br>12. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.<br>13. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.<br>14. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.<br>15. 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.<br>16. 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).<br>17. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.<br>18. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.<br>19. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.<br>20. 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.<br>21. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. |

| | | |
|---|---|---|
| | | 22. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.<br>23. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.<br>24. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.<br>25. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.<br>26. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.<br>27. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.<br>28. 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.<br>29. 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.<br>30. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.<br>31. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.<br>32. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.<br>33. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.<br>34. 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.<br>35. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z |

| | | |
|---|---|---|
| | | Internetu lub z bazy zapisanej na dysku.<br>36. 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 , urządzeń przenośnych oraz urządzeń dowolnego typu.<br>37. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.<br>38. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia.<br>39. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.<br>40. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.<br>41. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika<br>42. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).<br>43. Oprogramowanie musi posiadać zaawansowany skaner pamięci.<br>44. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.<br>45. 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.<br>46. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.<br>47. 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.<br>48. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.<br>49. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur. |

| | | |
|---|---|---|
| | | 50. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.<br>51. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http<br>52. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (roll back).<br>53. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).<br>54. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.<br>55. 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.<br>56. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.<br>57. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.<br>58. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.<br>59. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.<br>60. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.<br>**Ochrona przed spamem**<br>61. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.<br>62. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.<br>63. 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.<br>64. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam.<br>65. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam.<br>66. 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”.<br>67. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.<br><br>**Zapora osobista (personal firewall)**<br>68. Zapora osobista ma pracować jednym z 4 trybów:<br>• tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora<br>• tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo),<br>• tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany,<br>• tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji.<br>69. Program musi akceptować istniejące reguły w zaporze systemu zaproponowanej przez Wykonawcę w ofercie, zezwalające na ruch przychodzący<br>70. Możliwość tworzenia list sieci zaufanych.<br>71. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie<br>72. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.<br>73. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.<br>74. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.<br>75. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.<br>76. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.<br>77. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.<br>78. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.<br>79. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci |

| | | |
|---|---|---|
| | | 80. 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, konkretny interfejs sieciowy w systemie.<br>81. Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia.<br>82. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem.<br><br>**Kontrola dostępu do stron internetowych**<br>83. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.<br>84. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.<br>85. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.<br>86. 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.<br>87. Moduł musi posiadać także możliwość grupowania kategorii już istniejących.<br>88. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj.<br>89. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny.<br><br>**Ochrona serwera plików**<br>1. Wsparcie dla systemów zaproponowanych przez Wykonawcę w ofercie.<br>2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.<br>3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.<br>4. Wbudowana technologia do ochrony przed rootkitami i exploitami.<br>5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.<br>6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.<br>7. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy |

| | | |
|---|---|---|
| | | pomocy skrótu w menu kontekstowym.<br>8. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.<br>9. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.<br>10. Możliwość skanowania dysków sieciowych i dysków przenośnych.<br>11. Skanowanie plików spakowanych i skompresowanych.<br>12. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.<br>13. Aplikacja powinna wspierać mechanizm klastrowania.<br>14. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).<br>15. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.<br>16. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.<br>17. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia.<br>18. 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.<br>19. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.<br>20. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.<br>21. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.<br>22. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.<br>23. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.<br>24. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.<br>25. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.<br>26. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.<br>27. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).<br>28. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar |

| | | |
|---|---|---|
| | | dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.<br>29. 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.<br>30. 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 będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.<br>31. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.<br>32. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.<br>33. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.<br>34. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.<br>35. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.<br>36. Po instalacji systemu antywirusowego, 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.<br>37. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.<br>38. System antywirusowy 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.<br>39. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.<br>40. System antywirusowy 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. |

| | | |
|---|---|---|
| | | 41. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).<br>42. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.<br>43. Aplikacja musi wspierać skanowanie magazynu Hyper-V<br>44. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów<br>45. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).<br>46. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).<br>47. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.<br><br>**Administracja zdalna**<br>1. Serwer administracyjny musi oferować możliwość instalacji na systemach zaproponowanych przez Wykonawcę w ofercie.<br>2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).<br>3. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.<br>4. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.<br>5. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.<br>6. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.<br>7. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.<br>8. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.<br>9. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.<br>10. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny.<br>11. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.<br>12. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. |

| | | |
|---|---|---|
| | | 13. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.<br>14. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.<br>15. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.<br>16. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.<br>17. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.<br>18. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.<br>19. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.<br>20. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.<br>21. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.<br>22. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.<br>23. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.<br>24. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.<br>25. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej.<br>26. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.<br>27. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. |

| | | |
|---|---|---|
| | | 28. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.<br>29. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.<br>30. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.<br>31. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.<br>32. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.<br>33. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.<br>34. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.<br>35. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp.<br>36. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.<br>37. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.<br>38. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.<br>39. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.<br>40. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.<br>41. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.<br>42. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.<br>43. Serwer administracyjny musi oferować możliwość maksymalizacji |

| | | |
|---|---|---|
| | | wybranego elementu monitorującego.<br>44. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.<br>45. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.<br>46. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.<br>47. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.<br>48. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.<br>49. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.<br>50. Serwer administracyjny musi być wyposażona w machizm auto dopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.<br>51. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).<br>Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań. |
| 17 | Oprogramowanie biurowe | Pakiet biurowy musi zawierać co najmniej:<br>a) Edytortekstów,<br>b) Arkuszkalkulacyjny,<br>c) Narzędzie do przygotowania i prowadzeniaprezentacji,<br>d) Narzędziedozarządzaniapocztąelektroniczną,kalendarzamiizadaniami<br>Ogólne:<br>a) Interfejs w językupolskim,<br>b) wbudowana pomockontekstowa,<br>c) możliwość instalacji na dostarczonym sprzęcie i systemieoperacyjnym<br>Edytor tekstów:<br>a) konwersja, pełna edycja i zapis plików w formatach: txt, rtf, doc, docx, odt, xml (wraz z atrybutami),<br>b) edycja i formatowanie tekstu (m.in. tabel, obiektów graficznych, wzorów matematycznych, osadzania wykresów z arkuszakalkulacyjnego),<br>c) tworzenie szablonówdokumentów,<br>d) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego,<br>e) wbudowana biblioteka obiektów graficznych isymboli,<br>f) wbudowany mechanizm automatycznego sprawdzania pisowni oraz poprawności gramatycznej w ww.językach, |

| | | |
|---|---|---|
| | | g) edycja nagłówków I stopek,<br>h) automatyczne numerowanie rozdziałów, tabel irysunków,<br>i) automatycznetworzeniespisutreści,przypisówiodnośnikówdotekstu,<br>j) śledzenie wprowadzonychzmian,<br>k) zabezpieczenie plików hasłem (zarówno do odczytu jak iedycji),<br>l) tworzenie korespondencjiseryjnej,<br>m) tworzeniemakr,<br>n) podgląd graficzny oraz wydrukdokumentów<br>Arkusz kalkulacyjny:<br>a) konwersja, pełna edycja i zapis plików w formatach: txt, csv, xls, xlsx, xml (wraz z atrybutami),<br>b) tworzenie arkuszy kalkulacyjnych obejmujących dane tekstowe, liczbowe, walutowe, procentowe, ułamkowe orazczasowe,<br>c) tworzenie formuł obejmujących operacje: tekstowe, matematyczne, logiczne, statystyczne oraz operacje na danych finansowych iczasowych,<br>d) tworzenie formuł obejmujących: wyszukiwanie danych, operacje natabelach,<br>e) tworzenie i osadzania wykresów (m.in. punktowych, liniowych, kolumnowych, słupkowych, warstwowych, kołowych, 3D),<br>f) formatowanie warunkowe komórekarkusza,<br>g) śledzenie formuł oraz automatyczna weryfikacja ichpoprawności,<br>h) tworzenie tabelprzestawnych,<br>i) raporty z wykorzystaniem wyszukiwaniawarunkowego,<br>j) automatyczne filtrowaniadanych,<br>k) automatyczne pobieranie danych z zewnętrznych źródeł: plików tekstowych, plików XML, arkuszy kalkulacyjnych, bazdanych,<br>l) zapis wielu arkuszy w jednympliku,<br>m) tworzenie szablonówdokumentów,<br>n) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego,<br>o) tworzenie oraz edycji nagłówków istopek,<br>p) osadzanie:symboli,tabel,rysunków,obiektówgraficznychorazwzorów matematycznych,<br>q) zabezpieczenie plików hasłem (zarówno do odczytu jak iedycji),<br>r) tworzenie korespondencjiseryjnej,<br>s) tworzeniemakr,<br>t) podgląd graficzny oraz wydrukdokumentów,<br>Narzędzie do przygotowania i prowadzenia prezentacji:<br>a) konwersja,pełnaedycjaizapisplikówwformatach:ppt,pptx,odp,xml(wrazzatrybutami),<br>b) edycja i formatowanie tekstu (m.in. tabel, obiektów graficznych, wzorów matematycznych, osadzania wykresów z arkuszakalkulacyjnego),<br>c) tworzenie szablonówprezentacji,<br>d) tworzenie animacji dla pojedynczych elementów jak i całychslajdów,<br>e) wbudowana biblioteka obiektów graficznych isymboli,<br>f) elementy multimedialne (m.in. rysunków, obiektów graficznych, tabel, nagrań dźwiękowych orazfilmów), |

| | | |
|---|---|---|
| | | g) formatowanie tekstów, obiektów graficznych oraztabel,<br>h) umieszczanie notatek oraz podkładudźwiękowego,<br>i) wsparcie dla prowadzącego prezentacje (licznik czasu, obsługa projektora multimedialnego i konfiguracjidwumonitorowej),<br>j) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego,<br>k) wbudowany mechanizm automatycznego sprawdzania pisowni oraz poprawności gramatycznej w ww.językach,<br>l) tworzenie oraz edycji nagłówków istopek,<br>m) zabezpieczenie plików hasłem (zarówno do odczytu jak iedycji),<br>n) podgląd graficzny oraz wydruk dokumentów (z możliwością wydruku kilku slajdów na jednej stronie oraznotatkami),<br>Narzędzie do zarządzania pocztą elektroniczną, kalendarzami i zadaniami:<br>a) pełna obsługa plików w formacie.pst,<br>b) obsługa poczty elektronicznej w oparciu o protokoły: SMTP/MIME, SMTPS, POP3, POP3S, IMAP,<br>c) automatyczne filtrowaniepoczty,<br>d) edycja i formatowanie tekstuwiadomości,<br>e) tworzenie i obsługakatalogów,<br>f) tworzenie szablonówdokumentów,<br>g) tworzenie automatycznych reguł zarządzającychpocztą,<br>h) oznaczanie wybranej poczty zdefiniowanymiatrybutami,<br>i) importiobsługawielukalendarzy(wtymkalendarzyzdalnychwformaciei Cal),<br>j) udostępnianie kalendarza innymużytkownikom,<br>k) tworzenieizarządzaniezdarzeniami(zmożliwościąustawieniaprzypomnień),<br>l) automatyczne wysyłanie i odbieranie informacji ospotkaniach,<br>m) tworzenie i zarządzaniezadaniami,<br>n) tworzenieizarządzanielistąkontaktową(wtymtworzeniagrupodbiorców),<br>o) odbiór i wysyłanie elektronicznych wizytówek w formacievCard,<br>p) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego,<br>q) podgląd graficzny oraz wydruk dokumentów<br>Inne<br>Licencja dożywotnia na pakiet biurowy<br>Zamawiający nie dopuszcza pakietów biurowych , których użytkowanie wymaga okresowego wykupywania licencji na użytkowanie, tzw. opłaty abonamentowe |
| 18 | BIOS | BIOS zgodny ze specyfikacją UEFI<br>- Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o:<br>modelu komputera, PN, numerze seryjnym, Asset Tag, MAC Adres karty sieciowej, wersja Biosu wraz z datą produkcji, zainstalowanym procesorze, jego taktowaniu i ilości rdzeni, ilości pamięci RAM wraz z taktowaniem, stanie pracy wentylatora na procesorze, stanie pracy wentylatorów w obudowie komputera, napędach lub dyskach podłączonych do portów M.2 oraz SATA (model dysku twardego i napędu optycznego) |

| | | |
|---|---|---|
| | | Możliwość z poziomu Bios:<br>wyłączenia/włączenia selektywnego (pojedynczo) portów USB zarówno z przodu jak i z tyłu obudowy; wyłączenia kontrolera selektywnego (pojedynczego) portów SATA; konfiguracji kontrolera SATA; wyłączenia karty sieciowej, karty audio, portu szeregowego, wbudowanego głośnika, PXE; możliwość ustawienia portów USB w jednym z dwóch trybów:<br>1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB<br>2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej<br>ustawienia hasła: administratora, Power-On, HDD; blokady aktualizacji BIOS bez podania hasła administratora; wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów; alertowania zmiany konfiguracji sprzętowej komputera; wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan); ustawienia trybu wyłączenia komputera w stan niskiego poboru energii; zdefiniowania trzech sekwencji botujących (podstawowa, WOL, po awarii); załadowania optymalnych ustawień BIOS, obsługa BIOS za pomocą klawiatury i myszy bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. |
| 19 | Zintegrowany System Diagnostyczny | Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów:<br>• wykonanie testu pamięci RAM<br>• test dysku twardego<br>• test monitora<br>• test magistrali PCI-e<br>• test portów USB<br>• test płyty głównej<br>Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera.<br>Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie:<br>• PC: Producent, model<br>• BIOS: Wersja oraz data wydania Bios<br>• Procesor : Nazwa, taktowanie<br>• Pamięć RAM : Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci<br>• Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy<br>• Monitor: producent, model, rozdzielczość<br>System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera. |

| | | |
|---|---|---|
| 20 | Certyfikaty i standardy | - Certyfikat ISO9001:2000 dla producenta sprzętu<br>– ENERGY STAR 6.1<br>- Deklaracja zgodności CE<br>- Głośność jednostki mierzona z pozycji operatora z umiejscowieniem komputera na biurku w trybie IDLE 23 dB - dołączyć certyfikat lub dokument potwierdzający głośność jednostki<br>- Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki |
| 21 | Waga/rozmiary urządzenia | Waga urządzenia max. 7kg<br>Suma wymiarów nie może przekraczać: 735mm |
| 22 | Bezpieczeństwo i zdalne zarządzanie | - Złącze typu Kensington Lock umożliwiające zastosowanie zabezpieczenia fizycznego w postaci linki metalowej uniemożliwiającej również otwarcie obudowy<br>- Dedykowane oczko na kłódkę umożliwiającą zastosowanie zabezpieczenia fizycznego przed otwarciem obudowy<br>- Moduł TPM 2.0 |
| 23 | Oprogramowanie | Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. Oprogramowanie musi zapewniać również ustawienie automatycznego uaktualnienia wszystkich sterowników we wskazanym dniu miesiąca. |
| 24 | Gwarancja | Minimum 60 miesięcy świadczona w miejscu użytkowania sprzętu (on-site) z gwarantowanym czasem reakcji w następnym dniu roboczym. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.<br>Sprzęt musi być wyprodukowany nie wcześniej niż w II połowie 2017 roku. |
| 25 | Wsparcie techniczne producenta | Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. Możliwość weryfikacji na stronie producenta konfiguracji fabrycznej zakupionego sprzętu. Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |
| 26 | Dodatkowe | Przewód Patchcord UTP kategorii 6A, RJ 45 długość 3 metry, przewód zasilający, podkładka pod mysz |
| 27 | Inne | Dostawca rozpakuje, podłączy, uruchomi i skonfiguruje wszystkie stacje robocze w lokalizacji Zamawiającego w miejscach wskazanych przez Zamawiajacego |

**Monitor – 10 sztuk**

| L.p. | Parametr | Charakterystyka (wymagania minimalne) |
|---|---|---|

| | | |
|---|---|---|
| 1 | Przekątna ekranu i wymiary aktywnego obszaru wyświetlania | 21,5“ 476 mm x 268 mm |
| 2 | zalecana rozdzielczość | 1920 x 1080 (Full HD) |
| 3 | Typowy pobór mocy / w trybie Power management | 19 W / 0,5 W |
| 4 | złącza | VGA, HDMI |
| 5 | kontrast typowy | 600 : 1 |
| 6 | Kontrast dynamiczny | 10 000 000 : 1 |
| 7 | Jasność typowa | 200 cd/m2 |
| 8 | wielkość plamki | 0,248 mm |
| 9 | Czas reakcji | 5 ms |
| 10 | Kąt widzenia przy CR>10 | poziomo/pionowo: min. 90°/65° |
| 11 | Regulacja cyfrowa OSD | TAK |
| 12 | Certyfikaty i standardy | - CE,<br>- EnergyStar 6.0<br>- TCO<br>- EPEAT Silver |
| 13 | Gwarancja | Minimum 60 miesięcy. |
| 14 | Dodatkowe | Przewód zasilający, przewód do podłączenia monitora z komputerem |
| 15 | Inne | Dostawca rozpakuje, podłączy, uruchomi monitory w lokalizacji Zamawiającego w miejscach wskazanych przez Zamawiajacego |

**Stanowiska komputerowe laptopy – 5 sztuk**

| Lp. | Parametr | Charakterystyka (wymagania minimalne) |
|---|---|---|
| 1 | Komputer | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego notebooka. |
| 2 | Ekran | Matryca TFT 15,6” z podświetleniem w technologii LED, powłoka antyrefleksyjna Anti-Glare- rozdzielczość:<br>- HD 1366x768, 220nits, kontrast 350:1<br>Kąt otwarcia matrycy min.180 stopni. |
| 3 | Obudowa | Komputer wykonany z materiałów o podwyższonej odporności na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych, |

| | | |
|---|---|---|
| | | charakteryzujący się wzmocnioną konstrukcją, tzw. „business rugged”, według normy Mil-Std-810G tj. taki, który zaliczył (co najmniej) następujące testy z wynikiem pozytywnym:<br>· Uderzenia- Metoda 516.6<br>· Zmienna Temperatura- Metoda 503.5<br>· Wilgotność- Metoda 507.5<br>W celu potwierdzenia, że oferowana dostawa odpowiada wymaganiom określonym przez zamawiającego.<br>Oświadczenie Wykonawcy potwierdzone oświadczeniem lub innym dokumentem pochodzącym od producenta, potwierdzające, że komputer spełnia standardy MIL-STD-810G, i pozytywnie przeszedł testy w zakresie minimum wyżej wymienionych.<br>Komputer wyposażony w czujnik otwarcia obudowy zabezpieczający przed nieautoryzowanym dostępem. Praca czujnika konfigurowana z poziomu BIOS. |
| 4 | Chipset | Dostosowany do zaoferowanego procesora |
| 5 | Płyta główna | Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejsy SATA III (6 Gb/s), M.2 do obsługi dysków SATA lub WWAN. |
| 6 | Procesor | Procesor klasy x86, 2 rdzeniowy, zaprojektowany do pracy w komputerach przenośnych, taktowany zegarem co najmniej 2,4 GHz, pamięcią cache L3 co najmniej 3 MB lub równoważny wydajnościowo osiągający wynik co najmniej 3800 pkt w teście SysMark w kategorii PassMark CPU Mark, według wyników opublikowanych na stronie http://www.cpubenchmark.net |
| 7 | Pamięć operacyjna | Min 4GB z możliwością rozbudowy do 32GB, rodzaj pamięci DDR4, 2133MHz. Komputer wyposażony w minimum dwa banki pamięci umożliwiające pracę w trybie dual-channel. |
| 8 | Dysk twardy | Min 256GB SSD M.2 NVMe zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. |
| 9 | Napęd optyczny | Wbudowana nagrywarka DVD |
| 10 | Karta graficzna | Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki.<br>Karta graficzną osiągająca min. 930 pkt w teście Videocard Benchmark (http://www.videocardbenchmark.net/) |
| 11 | Audio/Video | Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo min 2x 1.5W, wbudowane dwa mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute), kamera HD720p pracująca przy niskim oświetleniu. |
| 12 | Karta sieciowa | 10/100/1000 – RJ 45 |
| 13 | Porty/złącza | 4xUSB 3.1 Gen 1 (jeden z możliwością ładowania urządzeń zewnętrznych poprzez port USB przy wyłączonym komputerze), złącze słuchawek i mikrofonu (combo), VGA, Mini Display Port, RJ-45, czytnik kart multimedialnych (min. SD/SDHC/SDXC/MMC), czytnik kart chipowych, dedykowane złącze dokowania umieszczone w spodniej części notebooka (nie dopuszcza się replikatora portów podłączanego poprzez port USB), Smart card reader. Złącze umożliwiające podpięcie linki antykradzieżowej. |

| | | |
|---|---|---|
| 14 | Dokowanie | Dedykowane złącze stacji dokującej dostępne od spodu notebooka, wyposażone w systemem chroniącym styki przed zanieczyszczeniem. |
| 15 | Klawiatura | Klawiatura odporna na zalanie, układ US, z wbudowanym trackpointem, touchpad z obsługą gestów. Klawiatura posiada wydzieloną część numeryczną. |
| 16 | WiFi | Wbudowana karta sieciowa, pracująca w standardzie AC 2x2 |
| 17 | Bluetooth | Wbudowany moduł Bluetooth 4.1 |
| 18 | Modem LTE | Możliwość rozbudowy notebooka o zintegrowany z obudową komputera modem LTE wraz ze slotem na kartę typu SIM (nie dopuszcza się modemów wykorzystujących Express Card oraz USB port) |
| 19 | Bateria | Notebook wyposażony baterie o pojemności min. 48 Wh<br>- pozwalające na nieprzerwaną pracę urządzenia do 14 godziny – załączyć test Mobile Mark 2014 lub kartę katalogową oferowanego komputera potwierdzającą czas pracy na zasilaniu bateryjnym. |
| 20 | Zasilacz | Zasilacz zewnętrzny maks. 45W |
| 21 | System operacyjny | System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:<br>1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:<br>a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,<br>b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych<br>2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego<br>3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim<br>4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.<br>5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe<br>6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,<br>7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.<br>8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim<br>9. Wbudowany system pomocy w języku polskim.<br>10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).<br>11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.<br>12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.<br>13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.<br>14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile |

| | | |
|---|---|---|
| | | użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.<br>15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.<br>16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".<br>17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.<br>18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.<br>19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.<br>20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.<br>21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.<br>22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.<br>23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."<br>24. Wbudowany mechanizm wirtualizacji typu hypervisor."<br>25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.<br>26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.<br>27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.<br>28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).<br>29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.<br>30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.<br>31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.<br>32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM<br>33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy |

| | | |
|---|---|---|
| | | odzyskiwania do szyfrowania dysku w usługach katalogowych.<br>34. Możliwość tworzenia wirtualnych kart inteligentnych.<br>35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)<br>36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.<br>37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.<br>38. Mechanizmy logowania w oparciu o:<br>a. Login i hasło,<br>b. Karty inteligentne i certyfikaty (smartcard),<br>c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),<br>d. Certyfikat/Klucz i PIN<br>e. Certyfikat/Klucz i uwierzytelnienie biometryczne<br>39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5<br>40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.<br>41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach<br>42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń<br>43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń |
| 22 | Oprogramowanie antywirusowe | 1. Pełne wsparcie dla systemu zaproponowanego przez Wykonawcę w ofercie– LICENCJA NA OKRES MINIMUM 60 MIESIĘCY<br>2. Wsparcie dla systemów posiadanych przez Zamawiającego na stanowiskach użytkowników, tzn. MS Windows: XP, Vista, 7, 8, 10<br>3. Wersja programu dla stacji roboczych dostępna zarówno w języku polskim jak i angielskim.<br>**Ochrona antywirusowa i antyspyware**<br>4. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.<br>5. Wbudowana technologia do ochrony przed rootkitami.<br>6. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.<br>7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.<br>8. 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.<br>9. 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<br>10. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.<br>11. Możliwość automatycznego wyłączenia komputera po zakończonym |

| | | |
|---|---|---|
| | | skanowaniu.<br>12. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.<br>13. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.<br>14. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.<br>15. 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.<br>16. 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).<br>17. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.<br>18. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.<br>19. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.<br>20. 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.<br>21. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.<br>22. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.<br>23. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.<br>24. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.<br>25. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.<br>26. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.<br>27. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. |

| | | |
|---|---|---|
| | | 28. 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.<br>29. 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.<br>30. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.<br>31. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.<br>32. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.<br>33. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.<br>34. 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.<br>35. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.<br>36. 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 , urządzeń przenośnych oraz urządzeń dowolnego typu.<br>37. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.<br>38. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia.<br>39. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.<br>40. W momencie podłączenia zewnętrznego nośnika aplikacja musi |

| | | |
|---|---|---|
| | | wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.<br>41. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika<br>42. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).<br>43. Oprogramowanie musi posiadać zaawansowany skaner pamięci.<br>44. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.<br>45. 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.<br>46. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.<br>47. 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.<br>48. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.<br>49. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.<br>50. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.<br>51. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http<br>52. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (roll back).<br>53. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).<br>54. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.<br>55. 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.<br>56. Wsparcie techniczne do programu świadczone w języku polskim przez |

| | | |
|---|---|---|
| | | polskiego dystrybutora autoryzowanego przez producenta programu.<br>57. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.<br>58. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.<br>59. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.<br>60. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.<br>**Ochrona przed spamem**<br>61. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.<br>62. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.<br>63. 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.<br>64. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam.<br>65. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam.<br>66. 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”.<br>67. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.<br><br>**Zapora osobista (personal firewall)**<br>68. Zapora osobista ma pracować jednym z 4 trybów:<br>• tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora<br>• tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo),<br>• tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany,<br>• tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory |

| | | |
|---|---|---|
| | | analizując aktywność sieciową danej stacji.<br>69. Program musi akceptować istniejące reguły w zaporze systemu zaproponowanej przez Wykonawcę w ofercie, zezwalające na ruch przychodzący<br>70. Możliwość tworzenia list sieci zaufanych.<br>71. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie<br>72. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.<br>73. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.<br>74. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.<br>75. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.<br>76. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.<br>77. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.<br>78. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.<br>79. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci<br>80. 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, konkretny interfejs sieciowy w systemie.<br>81. Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia.<br>82. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem.<br><br>**Kontrola dostępu do stron internetowych**<br>83. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.<br>84. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.<br>85. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.<br>86. 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.<br>87. Moduł musi posiadać także możliwość grupowania kategorii już istniejących.<br>88. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj.<br>89. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny.<br><br>**Ochrona serwera plików**<br>48. Wsparcie dla systemów zaproponowanych przez Wykonawcę w ofercie.<br>49. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.<br>50. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.<br>51. Wbudowana technologia do ochrony przed rootkitami i exploitami.<br>52. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.<br>53. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.<br>54. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.<br>55. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.<br>56. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.<br>57. Możliwość skanowania dysków sieciowych i dysków przenośnych.<br>58. Skanowanie plików spakowanych i skompresowanych.<br>59. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.<br>60. Aplikacja powinna wspierać mechanizm klastrowania.<br>61. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).<br>62. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.<br>63. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.<br>64. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia. |

| | | |
|---|---|---|
| | | 65. 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.<br>66. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.<br>67. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.<br>68. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.<br>69. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.<br>70. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.<br>71. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.<br>72. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.<br>73. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.<br>74. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).<br>75. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.<br>76. 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.<br>77. 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 będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.<br>78. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.<br>79. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.<br>80. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.<br>81. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.<br>82. System antywirusowy ma mieć możliwość kontroli zainstalowanych |

| | | |
|---|---|---|
| | | aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.<br>83. Po instalacji systemu antywirusowego, 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.<br>84. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.<br>85. System antywirusowy 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.<br>86. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.<br>87. System antywirusowy 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.<br>88. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).<br>89. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.<br>90. Aplikacja musi wspierać skanowanie magazynu Hyper-V<br>91. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów<br>92. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).<br>93. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).<br>94. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.<br><br>**Administracja zdalna**<br>52. Serwer administracyjny musi oferować możliwość instalacji na systemach zaproponowanych przez Wykonawcę w ofercie.<br>53. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).<br>54. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów |

| | | |
|---|---|---|
| | | oddzielnie bezpośrednio ze strony producenta.<br>55. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.<br>56. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.<br>57. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.<br>58. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.<br>59. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.<br>60. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.<br>61. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny.<br>62. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.<br>63. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.<br>64. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.<br>65. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.<br>66. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.<br>67. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.<br>68. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.<br>69. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.<br>70. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.<br>71. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.<br>72. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.<br>73. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. |

| | | |
|---|---|---|
| | | Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.<br>74. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.<br>75. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.<br>76. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej.<br>77. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.<br>78. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.<br>79. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.<br>80. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.<br>81. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.<br>82. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.<br>83. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.<br>84. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.<br>85. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.<br>86. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp.<br>87. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.<br>88. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.<br>89. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie |

| | | |
|---|---|---|
| | | będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.<br>90. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.<br>91. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.<br>92. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.<br>93. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.<br>94. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.<br>95. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.<br>96. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.<br>97. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.<br>98. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.<br>99. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.<br>100. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.<br>101. Serwer administracyjny musi być wyposażona w machizm auto dopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.<br>102. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).<br>103. Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań. |
| 23 | Oprogramowanie biurowe | Pakiet biurowy musi zawierać co najmniej:<br>a) Edytor tekstów,<br>b) Arkusz kalkulacyjny,<br>c) Narzędzie do przygotowania i prowadzenia prezentacji,<br>d) Narządziedozarządzaniapocztąelektroniczną,kalendarzamiizadaniami<br>Ogólne:<br>a) Interfejs w języku polskim, |

| | | |
|---|---|---|
| | | b) wbudowana pomoc kontekstowa,<br>c) możliwość instalacji na dostarczonym sprzęcie i systemie operacyjnym<br>Edytor tekstów:<br>a) konwersja, pełna edycja i zapis plików w formatach: txt, rtf, doc, docx, odt, xml (wraz z atrybutami),<br>b) edycja i formatowanie tekstu (m.in. tabel, obiektów graficznych, wzorów matematycznych, osadzania wykresów z arkuszakalkulacyjnego),<br>c) tworzenie szablonów dokumentów,<br>d) wbudowany słownik języka: polskiego, angielskiego oraz niemieckiego,<br>e) wbudowana biblioteka obiektów graficznych i symboli,<br>f) wbudowany mechanizm automatycznego sprawdzania pisowni oraz poprawności gramatycznej w ww. językach,<br>g) edycja nagłówków I stopek,<br>h) automatyczne numerowanie rozdziałów, tabel i rysunków,<br>i) automatyczne tworzenie spisu treści, przypisów i odnośników do tekstu,<br>j) śledzenie wprowadzonych zmian,<br>k) zabezpieczenie plików hasłem (zarówno do odczytu jak iedycji),<br>l) tworzenie korespondencji seryjnej,<br>m) tworzenie makr,<br>n) podgląd graficzny oraz wydruk dokumentów<br>Arkusz kalkulacyjny:<br>a) konwersja, pełna edycja i zapis plików w formatach: txt, csv, xls, xlsx, xml (wraz z atrybutami),<br>b) tworzenie arkuszy kalkulacyjnych obejmujących dane tekstowe, liczbowe, walutowe, procentowe, ułamkowe oraz czasowe,<br>c) tworzenie formuł obejmujących operacje: tekstowe, matematyczne, logiczne, statystyczne oraz operacje na danych finansowych i czasowych,<br>d) tworzenie formuł obejmujących: wyszukiwanie danych, operacje natabelach,<br>e) tworzenie i osadzania wykresów (m.in. punktowych, liniowych, kolumnowych, słupkowych, warstwowych, kołowych, 3D),<br>f) formatowanie warunkowe komórek arkusza,<br>g) śledzenie formuł oraz automatyczna weryfikacja ich poprawności,<br>h) tworzenie table przestawnych,<br>i) raporty z wykorzystaniem wyszukiwania warunkowego,<br>j) automatyczne filtrowania danych,<br>k) automatyczne pobieranie danych z zewnętrznych źródeł: plików tekstowych, plików XML, arkuszy kalkulacyjnych, bazdanych,<br>l) zapis wielu arkuszy w jednym pliku,<br>m) tworzenie szablonów dokumentów,<br>n) wbudowany słownik języka: polskiego, angielskiego oraz niemieckiego,<br>o) tworzenie oraz edycji nagłówków i stopek,<br>p) osadzanie:symboli,tabel,rysunków,obiektówgraficznychorazwzorówm |

| | | |
|---|---|---|
| | | atematycznych,<br>q) zabezpieczenie plików hasłem (zarówno do odczytu jak iedycji),<br>r) tworzenie korespondencji seryjnej,<br>s) tworzenie makr,<br>t) podgląd graficzny oraz wydruk dokumentów,<br>Narzędzie do przygotowania i prowadzenia prezentacji:<br>a) konwersja,pełnaedycjaizapisplikówwformatach:ppt,pptx,odp,xml(wrazzatrybutami),<br>b) edycja i formatowanie tekstu (m.in. tabel, obiektów graficznych, wzorów matematycznych, osadzania wykresów z arkusza kalkulacyjnego),<br>c) tworzenie szablonów prezentacji,<br>d) tworzenie animacji dla pojedynczych elementów jak i całych slajdów,<br>e) wbudowana biblioteka obiektów graficznych i symboli,<br>f) elementy multimedialne (m.in. rysunków, obiektów graficznych, tabel, nagrań dźwiękowych oraz filmów),<br>g) formatowanie tekstów, obiektów graficznych oraz tabel,<br>h) umieszczanie notatek oraz podkładu dźwiękowego,<br>i) wsparcie dla prowadzącego prezentacje (licznik czasu, obsługa projektora multimedialnego i konfiguracji dwumonitorowej),<br>j) wbudowany słownik języka: polskiego, angielskiego oraz niemieckiego,<br>k) wbudowany mechanizm automatycznego sprawdzania pisowni oraz poprawności gramatycznej w ww.językach,<br>l) tworzenie oraz edycji nagłówków i stopek,<br>m) zabezpieczenie plików hasłem (zarówno do odczytu jak i edycji),<br>n) podgląd graficzny oraz wydruk dokumentów (z możliwością wydruku kilku slajdów na jednej stronie oraz notatkami),<br>Narzędzie do zarządzania pocztą elektroniczną, kalendarzami i zadaniami:<br>a) pełna obsługa plików w formacie.pst,<br>b) obsługa poczty elektronicznej w oparciu o protokoły: SMTP/MIME, SMTPS, POP3, POP3S, IMAP,<br>c) automatyczne filtrowaniepoczty,<br>d) edycja i formatowanie tekstuwiadomości,<br>e) tworzenie i obsługakatalogów,<br>f) tworzenie szablonówdokumentów,<br>g) tworzenie automatycznych reguł zarządzającychpocztą,<br>h) oznaczanie wybranej poczty zdefiniowanymiatrybutami,<br>i) importiobsługawielukalendarzy(wtymkalendarzyzdalnychwformacieiCal),<br>j) udostępnianie kalendarza innymużytkownikom,<br>k) tworzenieizarządzaniezdarzeniami(zmożliwościąustawieniaprzypomnień),<br>l) automatyczne wysyłanie i odbieranie informacji ospotkaniach,<br>m) tworzenie i zarządzaniezadaniami,<br>n) tworzenieizarządzanielistąkontaktową(wtymtworzeniagrupodbiorców),<br>o) odbiór i wysyłanie elektronicznych wizytówek w formacievCard, |

| | | |
|---|---|---|
| | | p) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego,<br>q) podgląd graficzny oraz wydrukdokumentów.<br>Inne<br>Licencja dożywotnia na pakiet biurowy<br>Zamawiający nie dopuszcza pakietów biurowych , których użytkowanie wymaga okresowego wykupywania licencji na użytkowanie, tzw. opłaty abonamentowe |
| 24 | BIOS | BIOS zgodny ze specyfikacją UEFI.<br>Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji:wersji BIOS wraz z datą; nr seryjnym komputera; ilości pamięciami RAM; typie procesora i jego prędkości; MAC adresu zintegrowanej karty sieciowej; unikalnych nr inwentarzowych tzw. Asset Tag'ów; nr seryjnym płyty głównej komputera<br>Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:<br>- Możliwość Wyłączania/Włączania technologii antykradzieżowej<br>- Możliwość autentykacji użytkownika w BIOS z wykorzystaniem czytnika linii papilarnych<br>- Możliwość konfiguracji pracy czujnika otwarcia obudowy w taki sposób aby przy próbie otwarcia obudowy komputera i próbie jego uruchomienia pojawia się monit o podanie hasła supervisor'a zapisanego w BIOS.<br>- Możliwość ustawienia hasła dla twardego dysku<br>- Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password<br>- Możliwość ustawienia minimalnych wymagań dotyczących długości hasła POWER-On oraz hasła dysku twardego.<br>- Możliwość włączania/wyłączania wirtualizacji z poziomu BIOSU<br>- Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej.<br>- Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, mikrofonu, zintegrowanej kamery, portów USB, Czytnika kart chipowych, bluetooth<br>- Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie Administratora oraz możliwość ustawienia takiej zależności, że widok użytkownika pozwala na podgląd ustawień, ale nie ma możliwości wprowadzania zmian w BIOS.<br>- Możliwość niezależnego włączenia/wyłączenia płytki dotykowej oraz trackpointa<br>Możliwość ustawienia konieczności podania hasła Administratora przy próbie aktualizacji BIOS |
| 1. | Oprogramowanie dodatkowe | Oprogramowanie umożliwiające aktualizacje sterowników oraz podsystemu zabezpieczeń poprzez Internet.<br>Oprogramowanie do wykonania kopii bezpieczeństwa systemu operacyjnego i danych użytkownika na dysku twardym, zewnętrznych dyskach, sieci, CD-ROM-ie oraz ich odtworzenie po ewentualnej awarii systemu operacyjnego bez potrzeby jego reinstalacji. |

| | | |
|---|---|---|
| | | Oprogramowanie w wersji polskiej lub angielskiej. |
| 2. | Certyfikaty i standardy | - Certyfikat ISO9001:2000 dla producenta sprzętu<br>- Certyfikat EPEAT na poziomie co najmniej GOLD.<br>- ENERGY STAR 6.1<br>- Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z ww. systemem operacyjnym (wydruk ze strony Microsoft WHCL)<br>- Deklaracja zgodności CE<br>- Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki |
| 3. | Waga/Wymiary | Waga urządzenia z baterią podstawową max 2,5 kg, suma wymiarów urządzenia max 700 mm. |
| 4. | Szyfrowanie i bezpieczeństwo | Komputer wyposażony w moduł TPM 2.0<br>Notebook wyposażony w czujnik otwarcia obudowy zabezpieczający przed nieautoryzowanym dostępem do notebooka. Czujnik musi sygnalizować próbę nieautoryzowanego dostępu do wnętrza komputera. Praca czujnika konfigurowana z poziomu BIOS w ten sposób, że przy ustawionym haśle SUPERVISOR w przypadku nieautoryzowanego otwarcia obudowy hasło to będzie wymagane do podania przy próbie uruchomienia notebooka. Zamawiający uzna za równoważne dostarczenie linki zabezpieczającej typu Kensington zamykanej w taki sposób, że nie będzie możliwe otwarcie obudowy notebooka gdy linka zabezpieczająca zostanie umieszczona i zamknięta z wykorzystaniem kluczyka w dedykowanym slocie Kensington. |
| 5. | Gwarancja | Minimum 60 miesięcy świadczona w miejscu użytkowania sprzętu (on-site) z gwarantowanym czasem reakcji w następnym dniu roboczym.Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.<br>Sprzęt musi być wyprodukowany nie wcześniej niż w II połowie 2017 roku. |
| 6. | Wsparcie techniczne producenta | Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. Możliwość weryfikacji na stronie producenta konfiguracji fabrycznej zakupionego sprzętu. Możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji. Możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego. Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. |
| 7. | Dodatkowe | Zasilacz, przewód Patchcord UTP kategorii 6A, RJ 45, długość 3 metry, podkładka pod mysz |
| 8. | Inne | Dostawca rozpakuje, podłączy, uruchomi i skonfiguruje wszystkie laptopy w lokalizacji Zamawiającego w miejscach wskazanych przez Zamawiajacego |

**Urządzenie wielofunkcyjne A4 monochromatyczne (drukarka, skaner, kopiarka, fax) – 3 sztuki**

| L.p. | Parametr | Charakterystyka (wymagania minimalne) |
|---|---|---|
| 1 | Drukowanie | Szybkość drukowania- 33 str./min |

| | | |
|---|---|---|
| | | Szybkość druku dwustronnego- 18 str/min<br>Czas pierwszego wydruku- 6,5 sekund<br>Rozdzielczość- 1200 x 1200 dpi<br>Języki druku- PCL5e, PCL6, IBM-PPR, XPS<br>Zespół drukowania- Dupleks mechaniczny |
| 2 | Skanowanie | Rozdzielczość skanowania- 600 x 600 dpi<br>Szybkość skanowania- Do 6 s/stronę w kolorze, 2s/stronę w czerni<br>Głębia kolorów- Wejście 48 bit/Wyjście 24 bit<br>Podawanie dokumentów- Automatyczny podajnik dokumentów wraz z duplexem na 50 arkuszy, skaner płaski<br>Format- M-TIFF, PDF, XPS, JPEG, GIF, PNG<br>Książka adresowa- LDAP, 300 adresów e-mail, 20 grup adresowych<br>Skanowanie do- FTP, HTTP, E-mail, TWAIN, CIFS, pamięci USB, |
| 3 | Kopiowanie | Czas wykonania pierwszej kopii- 10 sekund<br>Szybkość kopiowania- do 33 kopii/min<br>Rozdzielczość kopiowania- do 600 x 600dpi<br>Zmniejszanie/powiększanie- Zoom 25-400%<br>Maksymalna liczba kopii- 99 |
| 4 | Faksowanie | Złącza- RJ11 x 2 (Line/Tel), PSTN, Linia PBX<br>Szybkość- ITU-T G3(Super G3) do 33,6kbps, do 2 s/str.<br>Szybkie wybieranie- 16 przycisków szybkiego wybierania, 300 numerów<br>Lista rozgłaszania- Maksimum 100<br>Pamięć stron- 4MB |
| 5 | Interfejs i oprogramowanie | Złącza- Port USB 2.0, Ethernet 10/100/1000BaseTX<br>Komunikacja bezprzewodowa-<br>Tak, moduł bezprzewodowej karty sieciowej wbudowanej w urządzenie.<br>Kompatybilność z systemami operacyjnymi zaproponowanymi przez Wykonawcę w ofercie<br>Dodatkowe oprogramowanie-<br>Oprogramowanie producenta drukarki lub równoważne do monitorowania wykorzystania urządzenia oraz nakładania ograniczeń posiadające następujące funkcje:<br>- funkcjonować w środowisku zaproponowanym przez Wykonawcę w ofercie;<br>- obsługiwać zarówno drukarki sieciowe (czyli podłączone do sieci Ethernet poprzez wbudowaną w drukarkę wewnętrzną kartę sieciową) jak i drukarki podłączone lokalnie (przez port USB i/lub LPT)<br>- podawać nazwy użytkowników (np. ich loginy) drukujących poszczególne wydruki;<br>- podawać nazwy drukowanych plików, liczbę stron, datę i godzinę przeprowadzenia danego wydruku;<br>- Oprogramowanie dla systemów posiadanych przez Zamawiającego na stanowiskach użytkowników, tzn. MS Windows: XP, Vista, 7, 8, 10 |
| 6 | Podawanie papieru | Pojemność papieru- Podajnik 1: 250 arkuszy 80 g/m2;<br>Podajnik uniwersalny: 100 arkuszy 80 g/m2;<br>Możliwość instalacji dodatkowego podajnika papieru o pojemności 530 arkuszy 80g/m2 |

| | | |
|---|---|---|
| | | Format papieru- Podajnik 1: A4, A5, B5, A6<br>Podajnik uniwersalny: A4, A5, B5, A6, Monarch, Com-9, Com-10, DL, C5, C6, Druk dwustronny: A4, B5<br>Gramatura papieru- Podajnik 1: 60 – 120 g/m2;<br>Druk dwustronny: 60 – 120 g/m2;<br>Podajnik uniwersalny: 60 – 120 g/m2<br>Podajnik skanera: 60 – 105 g/m2<br>Odbiornik papieru- Do 150 arkuszy stroną zadrukowaną do dołu |
| 7 | Pozostałe parametry techniczne: | Pamięć (RAM)- Standardowa pamięć RAM: 512 MB<br>Obciążenie- Maksymalne obciążenie do 60 000 stron miesięcznie |
| 8 | Wymaganie dodatkowe: | Gwarancja- minimum 60 miesięcy max zgodnie ze złożoną ofertą gwarancji producenta drukarki - naprawa w miejscu instalacji w ciągu 24h od daty zgłoszenia lub sprzęt zastępczy.<br>Wymagane dokumenty:<br>Oświadczenie producenta sprzętu, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.<br>Certyfikat ISO 9001:2008 producenta oferowanego sprzętu<br>Certyfikat ISO 140001:2004 producenta oferowanego sprzętu<br>Materiały eksploatacyjne-<br>Wymagana rozdzielność bębna i tonera.<br>Toner startowy na 2 tys. stron zgodnie z normą ISO/ISC 19752<br>Urządzenie dostarczone musi być fabrycznie nowe, skonfigurowane, gotowe do pracy wraz z tonerem(-ami) umożliwiającym wydruk przynajmniej 7 000 stron A4 przy pokryciu zgodnie z normą ISO/ISC 19752. Toner musi być tego samego producenta co drukarka, nie mogą być regenerowane. |
| 9 | Inne | Przewód zasilający, Przewód USB o długości 1,8 metra do podłączenia urządzenia z komputerem |

**Urządzenie wielofunkcyjne A4 kolorowe (drukarka, skaner, kopiarka, fax) – 3 sztuki**

| L.p. | Parametr | Charakterystyka (wymagania minimalne) |
|---|---|---|
| 1 | Drukowanie | Szybkość drukowania w A4- 26 str./min w kolorze, 30 str./min w mono<br>Czas pierwszego wydruku- 9 sekund<br>Rozdzielczość- 1200 x 600 dpi<br>Czcionki druku- 87 skalowanych czcionek PCL i 80 czcionek PostScript<br>Języki druku- PCL5c, PCL6, PostScript 3 (emulacja), IBM-PPR, XPS<br>Zespół drukowania- Dupleks mechaniczny |

| | | |
|---|---|---|
| 2 | Skanowanie | Rozdzielczość skanowania- 60 x 600 dpi<br>Szybkość skanowania- Do 26 str./min kolor, do 30 str./min w czerni<br>Głębia kolorów- Wejście 30 bit/Wyjście 24 bit<br>Podawanie dokumentów- Automatyczny podajnik dokumentów wraz z duplexem na 50 arkuszy, skaner płaski<br>Format- M-TIFF, PDF, XPS, JPEG,<br>Książka adresowa- LDAP lub 200 adresów e-mail i 20 grup adresowych<br>Skanowanie do- FTP, HTTP, E-mail, TWAIN, CIFS, pamięci USB |
| 3 | Kopiowanie | Czas wykonania pierwszej kopii- 14 sekund<br>Szybkość kopiowania- Do 26 str./min kolor, do 30 str./min w czerni<br>Rozdzielczość kopiowania- do 600 x 600dpi<br>Zmniejszanie/powiększanie- Zoom 25-400%<br>Maksymalna liczba kopii- 99 |
| 4 | Faksowanie | Złącza- RJ11 x 2 (Line/Tel), PSTN, Linia PBX<br>Szybkość- ITU-T G3(Super G3) do 33,6kbps, do 3 s/str.<br>Szybkie wybieranie- 16 przycisków szybkiego wybierania, 100 numerów<br>Lista rozgłaszania- Maksimum 100<br>Pamięć stron- 250 MB |
| 5 | Interfejs i oprogramowanie | Złącza- Port USB 2.0, Ethernet 10/100/1000BaseTX<br>Kompatybilność z systemami operacyjnymi zaproponowanymi przez Wykonawcę w ofercie;<br>Dodatkowe oprogramowanie-<br>Oprogramowanie producenta drukarki lub równoważne do monitorowania wykorzystania urządzenia oraz nakładania ograniczeń posiadające następujące funkcje:<br>- wymaga się aby aplikacja pracowała w środowisku zaproponowanym przez Wykonawcę w ofercie;<br>- aplikacja powinna obsługiwać zarówno drukarki sieciowe (czyli podłączone do sieci Ethernet poprzez wbudowaną w drukarkę wewnętrzną kartę sieciową) jak i drukarki podłączone lokalnie (przez port USB i/lub LPT),<br>- aplikacja powinna rejestrować nazwy użytkowników (np. ich loginy) drukujących poszczególne wydruki;<br>- aplikacja powinna rejestrować i w ramach raportów podawać nazwy drukowanych plików, liczbę stron, datę i godzinę przeprowadzenia danego wydruku;<br>- w przypadku współpracy z urządzeniami kolorowymi w ramach funkcji ograniczenia dostępu aplikacja powinna mieć możliwość blokowania druku kolorowego (a w przypadku urządzeń wielofunkcyjnych kopii kolor)<br>- aplikacja lub dostarczone urządzenia powinny mieć możliwość automatycznej konwersji drukowanych plików na postać czarno-biała dla użytkowników z założoną blokadą druku w kolorze;<br>- Oprogramowanie dla systemów posiadanych przez Zamawiającego na stanowiskach użytkowników, tzn. MS Windows: XP, Vista, 7, 8, 10 |

| | | |
|---|---|---|
| 6 | Podawanie papieru | Pojemność papieru-<br>Podajnik 1: 250 arkuszy 80 g/m2;<br>Podajnik uniwersalny: 100 arkuszy 80 g/m2;<br>Podajnik skanera: 50 arkuszy 80 g/m2;<br>Możliwość instalacji dodatkowego podajnika papieru o pojemności 530 arkuszy 80g/m2<br>Format papieru-<br>Podajnik 1: A4, A5, B5, A6<br>Podajnik uniwersalny: A4, A5, B5, A6, Monarch, Com-9, Com-10, DL, C5, nośniki (baner) do 130 cm długości<br>Druk dwustronny: A4, B5, A5<br>Gramatura papieru-<br>Podajnik 1: 64 – 176 g/m2;<br>Druk dwustronny: 64 – 176 g/m2;<br>Podajnik uniwersalny: 64 – 220 g/m2<br>Podajnik skanera: 60 – 105 g/m2<br>Odbiornik papieru-<br>Do 150 arkuszy stroną zadrukowaną do dołu<br>D0 100 arkuszy stroną zadrukowaną do góry |
| 7 | Pozostałe parametry techniczne: | Pamięć (RAM)- Standardowa pamięć RAM: 1GB<br>Szybkość procesora- 660 MHz<br>Obciążenie- Maksymalne obciążenie do 45 000 stron miesięcznie |
| 8 | Wymaganie dodatkowe: | Gwarancja- minimum 60 miesięcy max zgodnie ze złożoną ofertą producenta drukarki.<br>Wymagane dokumenty:<br>Oświadczenie producenta sprzętu, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.<br>Certyfikat ISO 9001:2008 producenta oferowanego sprzętu<br>Certyfikat ISO 14001:2004 producenta oferowanego sprzętu<br>Materiały eksploatacyjne-<br>Wymagana rozdzielność bębna i tonera.<br>Tonery startowe na 1 tys. stron (toner czarny i tonery kolorowe) zgodnie z normą ISO/ISC 19752 oraz normą ISO/IEC 19798.<br>Urządzenie dostarczone musi być fabrycznie nowe, skonfigurowane, gotowe do pracy wraz z tonerem(-ami). |
| 9 | Inne | Przewód zasilający, Przewód USB o długości 1,8 metra do podłączenia urządzenia z komputerem |

**Oprogramowanie biurowe – 25 licencji**

| | | |
|---|---|---|
| | Oprogramowanie biurowe | Pakiet biurowy musi zawierać co najmniej:<br>a) Edytortekstów,<br>b) Arkuszkalkulacyjny,<br>c) Narzędzie do przygotowania i prowadzeniaprezentacji,<br>d) Narządziedozarządzaniapocztąelektroniczną,kalendarzamiizadaniami |

| | | |
|---|---|---|
| | | Ogólne:<br>a) Interfejs w językupolskim,<br>b) wbudowana pomockontekstowa,<br>c) możliwość instalacji na dostarczonym sprzęcie i systemieoperacyjnym<br>Edytor tekstów:<br>a) konwersja, pełna edycja i zapis plików w formatach: txt, rtf, doc, docx, odt, xml (wraz z atrybutami),<br>b) edycja i formatowanie tekstu (m.in. tabel, obiektów graficznych, wzorów matematycznych, osadzania wykresów z arkuszakalkulacyjnego),<br>c) tworzenie szablonówdokumentów,<br>d) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego,<br>e) wbudowana biblioteka obiektów graficznych isymboli,<br>f) wbudowany mechanizm automatycznego sprawdzania pisowni oraz poprawności gramatycznej w ww.językach,<br>g) edycja nagłówków I stopek,<br>h) automatyczne numerowanie rozdziałów, tabel irysunków,<br>i) automatycznetworzeniespisutreści,przypisówiodnośnikówdotekstu,<br>j) śledzenie wprowadzonychzmian,<br>k) zabezpieczenie plików hasłem (zarówno do odczytu jak iedycji),<br>l) tworzenie korespondencjiseryjnej,<br>m) tworzeniemakr,<br>n) podgląd graficzny oraz wydrukdokumentów<br>Arkusz kalkulacyjny:<br>a) konwersja, pełna edycja i zapis plików w formatach: txt, csv, xls, xlsx, xml (wraz z atrybutami),<br>b) tworzenie arkuszy kalkulacyjnych obejmujących dane tekstowe, liczbowe, walutowe, procentowe, ułamkowe orazczasowe,<br>c) tworzenie formuł obejmujących operacje: tekstowe, matematyczne, logiczne, statystyczne oraz operacje na danych finansowych iczasowych,<br>d) tworzenie formuł obejmujących: wyszukiwanie danych, operacje natabelach,<br>e) tworzenie i osadzania wykresów (m.in. punktowych, liniowych, kolumnowych, słupkowych, warstwowych, kołowych, 3D),<br>f) formatowanie warunkowe komórekarkusza,<br>g) śledzenie formuł oraz automatyczna weryfikacja ichpoprawności,<br>h) tworzenie tabelprzestawnych,<br>i) raporty z wykorzystaniem wyszukiwaniawarunkowego,<br>j) automatyczne filtrowaniadanych,<br>k) automatyczne pobieranie danych z zewnętrznych źródeł: plików tekstowych, plików XML, arkuszy kalkulacyjnych, bazdanych,<br>l) zapis wielu arkuszy w jednympliku,<br>m) tworzenie szablonówdokumentów,<br>n) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego,<br>o) tworzenie oraz edycji nagłówków istopek,<br>p) osadzanie:symboli,tabel,rysunków,obiektówgraficznychorazwzorów |

| | | |
|---|---|---|
| | | matematycznych,<br>q) zabezpieczenie plików hasłem (zarówno do odczytu jak iedycji),<br>r) tworzenie korespondencjiseryjnej,<br>s) tworzeniemakr,<br>t) podgląd graficzny oraz wydrukdokumentów,<br>Narzędzie do przygotowania i prowadzenia prezentacji:<br>a) konwersja,pełnaedycjaizapisplikówwformatach:ppt,pptx,odp,xml(wrazzatrybutami),<br>b) edycja i formatowanie tekstu (m.in. tabel, obiektów graficznych, wzorów matematycznych, osadzania wykresów z arkuszakalkulacyjnego),<br>c) tworzenie szablonówprezentacji,<br>d) tworzenie animacji dla pojedynczych elementów jak i całychslajdów,<br>e) wbudowana biblioteka obiektów graficznych isymboli,<br>f) elementy multimedialne (m.in. rysunków, obiektów graficznych, tabel, nagrań dźwiękowych orazfilmów),<br>g) formatowanie tekstów, obiektów graficznych oraztabel,<br>h) umieszczanie notatek oraz podkładudźwiękowego,<br>i) wsparcie dla prowadzącego prezentacje (licznik czasu, obsługa projektora multimedialnego i konfiguracjidwumonitorowej),<br>j) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego,<br>k) wbudowany mechanizm automatycznego sprawdzania pisowni oraz poprawności gramatycznej w ww.językach,<br>l) tworzenie oraz edycji nagłówków istopek,<br>m) zabezpieczenie plików hasłem (zarówno do odczytu jak iedycji),<br>n) podgląd graficzny oraz wydruk dokumentów (z możliwością wydruku kilku slajdów na jednej stronie oraznotatkami),<br>Narzędzie do zarządzania pocztą elektroniczną, kalendarzami i zadaniami:<br>a) pełna obsługa plików w formacie.pst,<br>b) obsługa poczty elektronicznej w oparciu o protokoły: SMTP/MIME, SMTPS, POP3, POP3S, IMAP,<br>c) automatyczne filtrowaniepoczty,<br>d) edycja i formatowanie tekstuwiadomości,<br>e) tworzenie i obsługakatalogów,<br>f) tworzenie szablonówdokumentów,<br>g) tworzenie automatycznych reguł zarządzającychpocztą,<br>h) oznaczanie wybranej poczty zdefiniowanymiatrybutami,<br>i) importiobsługawielukalendarzy(wtymkalendarzyzdalnychwformaciei Cal),<br>j) udostępnianie kalendarza innymużytkownikom,<br>k) tworzenieizarządzaniezdarzeniami(zmożliwościąustawieniaprzypomnień),<br>l) automatyczne wysyłanie i odbieranie informacji ospotkaniach,<br>m) tworzenie i zarządzaniezadaniami,<br>n) tworzenieizarządzanielistąkontaktową(wtymtworzeniagrupodbiorców),<br>o) odbiór i wysyłanie elektronicznych wizytówek w formacievCard,<br>p) wbudowanysłownikjęzyka:polskiego,angielskiegoorazniemieckiego, |

| | | |
|---|---|---|
| | | q) podgląd graficzny oraz wydruk dokumentów<br>Inne<br>Licencja dożywotnia na pakiet biurowy<br>Zamawiający nie dopuszcza pakietów biurowych , których użytkowanie wymaga okresowego wykupywania licencji na użytkowanie, tzw. opłaty abonamentowe |

**Przełącznik dostępowy - 3 szt.**

| L.p. | Parametr | Charakterystyka (wymagania minimalne) |
|---|---|---|
| 1 | Obudowa | Obudowa urządzenia musi być przystosowana do montażu w szafie 19” |
| 2 | Interfejsy | Minimum<br>- 24 x GbE RJ-45 porty<br>- 4 x 10 GbE SFP + sloty |
| 3 | Warstwa przełącznika | L2/L3 |
| 4 | Wydajność | - pojemność przełączania nie mniejsza niż 128 Gbps<br>- Prędkość przesyłania nie mniejsza niż 95 Mbps<br>- Bufor pakietu nie mniejszy niż 1500KB<br>Tabele adresów MAC nie miejsze niż 16K<br>Jumbo frame nie mniejsze niż 12KB |
| 5 | Zgodność ze standardami | - IEEE 802.3 – 10BaseT<br>- IEEE 802.3u – 100Base TX<br>- IEEE 803ab – 1000BaseT<br>- IEEE 80.3ae – 10-Gigabit Ethernet<br>- IEEE 802.3x flow control<br>- IEEE 80ad LACP aggregation<br>- IEEE 802.1D Spanning Tree Protocol (STP)<br>- IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)<br>- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)<br>- IEEE 802.1Q VLAN Tagging<br>- IEEE 802.1p Class Of Service (CoS) Prioritization |
| 6 | Odporność i dostępność | - dual images<br>- ERSP |
| 7 | Bezpieczeństwo | - 802.1X<br>- Port Security<br>- RADIUS serves<br>- Login authentication by RADIUS<br>- Login authentication by TACACS+<br>- SSH<br>- DHCP snooping<br>- ARP Inspection<br>- Static IP/MAC binding<br>- Guest VLAN<br>- ACL Packet Felitering (IPc4/IPv6) |
| 8 | Zarządzanie ruchem i QoS | - 802.1p<br>802.3x flow control |
| 9 | Zarządzanie urządzeniem | - Web interface |

| | | |
|---|---|---|
| | | - onsola, telnet, SNMP |
| 10 | Zużycie prądu | Powyżej 25W |
| 11 | Gwarancja | Urządzeniu powinno być objęte minimum 5 letnią gwarancją producenta |
| 12 | Serwis | W przypadku awarii urządzenia wysyłka zastępczego produktu następuje w tym samym dniu roboczym, w którym zostanie zgłoszona awaria. Urządzenie powinno być objęte w/w opcją serwisową w okresie nie krótszym niż 5 lat. |
| 13 | Dodatkowe wyposażenie | Wraz z przełącznikami dostarczyć i zamontować dwa moduły światłowodowych SFP-1GbE do światłowodu jednomodowego oraz dostarczyć i zamontować dwa kable do połączenia bezpośredniego SFP+ DO SFP+(10gBe) |
| 14 | Inne | Dostawca rozpakuje, zamontuje w szafie rack, uruchomi i skonfiguruje przełączniki w lokalizacji Zamawiającego w miejscach wskazanych przez Zamawiajacego |

**Zestawy komputerowe - 2szt**

Wykonawca w ramach realizacji przedmiotu zamówienia dostarczy Zamawiającemu 2 komputery allInOne wraz z czytnikami kodów kreskowych. Zestawy mają służyć do potwierdzania zabiegów fizjoterapeutycznych, muszą współpracować z dostarczonym przez Wykonawcę Oprogramowaniem Aplikacyjnym (**Zamawiający posiada oprogramowanie Mediqus Firmy Gabos).** Wykonawca dostarczy niezbędną ilość licencji dostępowych do współpracy dostarczonych komputerów z Oprogramowaniem Aplikacyjnym

**Wymagania szczegółowe dla komputerów – 2 szt.**
Wykonawca dostarczy 2 komputery AllInOne spełniających wymagania przedstawione w poniższej tabeli:

**Wymagane parametry techniczne dla komutera allInOne**

| Lp. | Parametr | Wymagana wartość parametru |
|---|---|---|
| 1. | Monitor | a) Przekątna - co najmniej: 15”<br>b) Rozdzielczość – co najmniej: 1366x 768 pikseli<br>c) Ekran dotykowy |
| 2. | Procesor | d) Co najmniej: 1,6 GHz |
| 3. | Pamięć RAM | e) Co najmniej: 4 GB |
| 4. | Dysk SSD | f) Co najmniej: 128GB |
| 5. | Złącza ( co najmniej) | g) USB 2.0 – 2szt.<br>h) USB 3.0 – 2 szt.<br>i) HDMI – 1szt.<br>j) VGA – 1 szt.<br>k) Czytnik kart pamięci – 1 szt.<br>l) Wyjście mikrofonowe |

| | | |
|---|---|---|
| | | m) Wyjście audio |
| 6. | Komunikacja | n) WI-fi: 802.11b/g/n<br>o) Karta sieciowa zintegrowana 10/100/1000 Mbit/s<br>p) Bluetooth – 1 szt. |
| 7. | Wyposażenie | q) klawiatura,<br>r) mysz,<br>s) przewód zasilający<br>t) instrukcja obsługi,<br>u) karta gwarancyjna |
| 8. | System operacyjny | v) System operacyjny współpracujący z dostarczonym Oprogramowaniem Aplikacyjnym – zgodnie z przeznaczeniem. |
| 9. | Gwarancja | w) minimum 60 miesięcy |
| 10. | Inne | x) Dostawca rozpakuje, podłączy, uruchomi i skonfiguruje komputery all in onew lokalizacji Zamawiającego w miejscach wskazanych przez Zamawiajacego |

**Wymagania szczegółowe dla czytnika kodów kreskowych – 2 szt.**
Dwa czytniki kodów kreskowych spełniających wymagania przedstawione w poniższej tabeli:

| Lp. | Parametr | Wymagana minimalna wartość parametru |
|---|---|---|
| 1. | Obsługiwane kody kreskowe | a) 1D |
| 2. | Gwarancja producenta [mc] | b) 60 |
| 3. | Dostępne interfejsy | c) USB, RS232, PS/2 |
| 4. | Kabel komunikacyjny | d) USB |
| 5. | Maks. odległość odczytu [cm] | e) 43 |
| 6. | Technologia odczytu | f) laser jednoliniowy |
| 7. | Temperatura pracy | g) od 0°C do 50°C |
| 8. | Bezpieczny upadek na twardą pow. [m] | h) 1.5 |
| 9. | Sygnalizacja | i) dźwiękowa |
| 10. | Wymiary [mm] | j) 152 x 64 x 85 |
| 11. | Temperatura składowania | k) od -40°C do 70°C |
| 12. | Dopuszczalna wilgotność otoczenia [%] | l) od 5% do 95% |
| 13. | Gwarancja | m) Minimum 60miesięcy |

**Modułu potwierdzania zabiegów fizjoterapeutycznych/rehabilitacyjnych**
Oprogramowanie musi posiadać moduł potwierdzania zabiegów fizjoterapeutycznych /rehabilitacyjnych, który stanowić będzie integralną część Oprogramowania Aplikacyjnego posiadanego przez Zamawiającego (system Mediqus firmy Gabos) , tj. będzie korzystał ze wspólnej bazy pacjentów, rejestracji, personelu itp. W/w moduł będzie służył do realizacji automatyzacji zabiegów fizjoterapeutycznych /rehabilitacyjnych. Realizacja pozycji zleceń zabiegów będzie odbywała się na specjalnych stanowiskach komputerowym.

Sposób realizacji pozycji zleceń:

1) realizacja pozycji zlecenia za pomocą kodu kreskowego, dotyku bez potrzeby wybierania ręcznego pacjenta, zlecenia
2) automatyczne dopisywanie procedur (w tym procedur zależnych od parametrów zlecenia),produktów podczas realizacji zabiegów,

identyfikacja pacjenta po kodzie kreskowym (opaska lub skierowanie)

Dostawca zainstaluje, kompleksowo skonfiguruje i zintegruje dostarczony Moduł potwierdzania zabiegów fizjoterapeutycznych/rehabilitacyjnych z systemem posiadanym przez Zamawiającego.
Dostawca dostarczy licencję do tego modułu na nieograniczoną liczbą użytkowników.
Zamawiający na dostarczony Moduł zamówienia w zakresie oprogramowania wymaga gwarancji, wsparcia technicznego i aktualizacji na okres minimum 60 miesięcy.

Zamawiający informuje, że tam, gdzie opisał przedmiot zamówienia przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, co mogłoby doprowadzić do uprzywilejowania lub wyeliminowania niektórych Wykonawców lub produktów, Zamawiający dopuszcza rozwiązanie równoważne opisywanym pod warunkiem, że będą one o nie gorszych właściwościach i jakości. Tam, gdzie Zamawiający opisał przedmiot zamówienia przez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa wart. 30 ust. 1 pkt 2 i ust. 3 ustawy PZP, Zamawiający wskazuje, że dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy, usługi lub roboty budowlane spełniają wymagania określone przez Zamawiającego.

1. Oferowane modele komputerów muszą posiadać certyfikat Microsoft, potwierdzający poprawną współpracę oferowanych modeli komputerów z ww. systemem operacyjnym (wydruk ze strony Microsoft WHCL).- stanowiska komputerowe laptopy
2. Deklaracja zgodności CE - stanowiska komputerowe laptopy
3. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki. - stanowiska komputerowe laptopy

4. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.- stanowiska komputerowe laptopy

5. Certyfikat ISO 9001:2008 dla producenta oferowanego sprzętu – drukarka laserowa

6. Certyfikat ISO 140001:2004 dla producenta oferowanego sprzętu. – drukarka laserowa

7. Oświadczenie producenta sprzętu, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. – urządzenie wielofunkcyjne A4 monochromatyczne

8. Certyfikat ISO 9001:2008 producenta oferowanego sprzętu – urządzenie wielofunkcyjne A4 monochromatyczne

9. Certyfikat ISO 140001:2004 producenta oferowanego sprzętu – urządzenie wielofunkcyjne A4 monochromatyczne

10. Oświadczenie producenta sprzętu, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem – urządzenie wielofunkcyjne A4 kolorowe 29. Certyfikat ISO 9001:2008 producenta oferowanego sprzętu – urządzenie wielofunkcyjne A4 kolorowe

11. Certyfikat ISO 14001:2004 producenta oferowanego sprzętu – urządzenie wielofunkcyjne A4 kolorowe

***ROZDZIAŁ III***

***UMOWA - WZÓR***

PCMG/P-36/2017

**UMOWA /wzór/**

**na zakup, instalację, uruchomienie urządzeń teleinformatycznych i oprogramowania w zakresie objętym projektem pn. „Poprawa jakości i dostępności świadczeń zdrowotnych dzięki wdrożeniu e-usług w Powiatowym Centrum Medycznym w Grójcu”**

Zawarta w dniu …… 2018 roku pomiędzy:
**Powiatowe Centrum Medyczne w Grójcu spółka z ograniczoną odpowiedzialnością** z siedzibą **w Grójcu** przy ulicy **Piotra Skargi 10,** wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy, XIV Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr 0000351118, NIP 7972019261 reprezentowaną przez:
Marzenę Barwicką – Prezesa Zarządu
(zwanym dalej „Zamawiającym”)
a **…… z siedzibą w …….. przy ulicy ……** wpisaną do rejestru przedsiębiorców prowadzonego przez …… pod nr ……., NIP ……reprezentowaną przez:
**……..**
(zwaną dalej “Wykonawcą”)

**w wyniku przeprowadzenia postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego poniżej 221 000 Euro na podst. art. 39 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jedn. Dz. U. z 2015r. poz. 2164 ze zm.), o następującej treści:**

**§ 1.**

**Przedmiot umowy, okres obowiązywania**

1. Na podstawie umowy Wykonawca zobowiązuje się dostarczyć Zamawiającemu i przenieść na Zamawiającego własność sprzętu będącego przedmiotem umowy, a Zamawiający zobowiązuje się sprzęt odebrać i zapłacić Wykonawcy cenę za jego dostarczenie.
2. Termin realizacji umowy **– do 4 tygodni od daty zawarcia umowy.**
3. Integralną część umowy stanowi wybrana oferta wraz wypełnioną specyfikacją techniczną.

**§ 2.**

**Warunki dostawy**

1. Korzyści i ciężary związane ze sprzętem oraz niebezpieczeństwo przypadkowej utraty lub uszkodzenia sprzętu przechodzą na Zamawiającego z chwilą wydania sprzętu Zamawiającemu lub osobie trzeciej wskazanej na piśmie przez Zamawiającego.
2. Osobą odpowiedzialną ze strony Zamawiającego w sprawie realizacji umowy jest **…….**
3. Osobą odpowiedzialną ze strony Wykonawcy w sprawie realizacji umowy jest **…….**

**§ 3.**

**Wydanie sprzętu, ubezpieczenie i transport**

1. Za dzień wydania sprzętu Zamawiającemu uważa się dostarczenie sprzętu, jego montaż, zainstalowanie, uruchomienie sprzętu oraz przeszkolenie personelu i po wykonaniu tych czynności protokolarne przejęcie przez Zamawiającego. Za miejsce dostawy (dalej Miejsce Dostawy) uznaje się adres **Odbiorcy:** ulica **Piotra Skargi 10, 05-600 Grojec.**

2. Wykonawca zapewni takie opakowanie sprzętu, jakie jest wymagane, aby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do Miejsca Dostawy.
3. Rodzaj i jakość wymaganego opakowania określają stosowne normy techniczne, a w przypadku braku takich norm, wszelkie znane Wykonawcy okoliczności dotyczące warunków transportu sprzętu do Miejsca Dostawy oraz warunków, jakich można się spodziewać w Miejscu Dostawy.
4. Do sprzętu Wykonawca dołączy specyfikacje, ulotkę w języku polskim zawierającą wszystkie niezbędne dla bezpośredniego użytkownika informacje oraz instrukcję obsługi w wersji papierowej i elektronicznej w języku polskim.

**§ 4.**

**Rękojmia za wady fizyczne i prawne**

1. Wykonawca jest odpowiedzialny względem Zamawiającego za wszelkie wady fizyczne dostarczonego sprzętu.
2. Przez wadę fizyczną rozumie się w szczególności jakąkolwiek niezgodność sprzętu z opisem przedmiotu zamówienia zawartym w zapytaniu ofertowym.
3. Wykonawca jest odpowiedzialny względem Zamawiającego za wszelkie wady prawne dostarczonego sprzętu, w tym również za ewentualne roszczenia osób trzecich wynikające z naruszenia praw własności intelektualnej lub przemysłowej, w tym praw autorskich, patentów, praw ochronnych na znaki towarowe oraz praw z rejestracji na wzory użytkowe i przemysłowe, pozostające w związku z wprowadzeniem towaru do obrotu na terytorium Rzeczypospolitej Polskiej.

**§ 5.**

**Gwarancja jakości, reklamacje**

1. Wykonawca gwarantuje Zamawiającemu, że dostarczony sprzęt w ramach umowy jest wolny od wad fizycznych w rozumieniu § 4, ust. 2 niniejszej umowy. Zamawiający może wykonywać uprawnienia z tytułu gwarancji niezależnie od uprawnień z tytułu rękojmi za wady fizyczne dostarczonego sprzętu.
2. Wykonawca wyda Zamawiającemu jednocześnie ze sprzętem dokument gwarancyjny co do jakości dostarczonego sprzętu, wystawiony przez siebie lub osobę trzecią.
3. Za okazaniem dokumentu gwarancyjnego Zamawiający może żądać od Wykonawcy lub innego gwaranta albo osób przez nich upoważnionych, naprawy lub wymiany sprzętu na wolny od wad. Wykonawca lub inny gwarant albo osoby przez nich upoważnione, zobowiązani są dokonać naprawy lub wymiany sprzętu.
4. Czas naprawy sprzętu wynosi nie dłużej niż 3 dni robocze. W przypadku braku możliwości szybkiej naprawy sprzętu Wykonawca zobowiązany jest zapewnić sprzęt zastępczy na czas naprawy wynoszący powyżej 3 dni roboczych.
5. Termin obowiązywania pełnej gwarancji na dostarczony sprzęt wynosi **…….. miesięcy** liczony od daty protokołu odbioru sprzętu. W okresie trwania gwarancji – okresowe bezpłatne przeglądy sprzętu nie rzadziej niż 1 raz w roku wraz z wymianą części zużywalnych przewidzianych przez producenta w procedurze przeglądowej. W tym okresie Zamawiający nie ponosi żadnych dodatkowych kosztów związanych z naprawą lub wymianą sprzętu z zastrzeżeniem ust. 6 niniejszego paragrafu.
6. Odpowiedzialność z tytułu gwarancji jakości obejmuje zarówno wady powstałe z przyczyn tkwiących w sprzęcie w chwili dokonania jego odbioru przez Zamawiającego, jak i wszelkie inne wady fizyczne sprzętu, powstałe z przyczyn, za które Wykonawca lub inny gwarant ponosi odpowiedzialność, pod

warunkiem, że wady te ujawnią się w ciągu terminu obowiązywania gwarancji. Podczas trwania gwarancji Wykonawca zobowiązuje się do bezpłatnej naprawy lub wymiany sprzętu określonego w umowie. Termin reakcji na zgłoszenie usunięcia wady nie może przekroczyć **48 godz**. od momentu zgłoszenia w dni robocze.

7. Wykonawca nie ponosi odpowiedzialności za uszkodzenia i wynikające z nich przestoje, jeżeli będą one spowodowane błędną obsługą, bądź nie stosowaniem się do instrukcji obsługi sprzętu określonego w umowie.

8. Jeśli Wykonawca lub gwarant albo osoba przez nich upoważniona, po wezwaniu ich do naprawy lub wymiany sprzętu i okazaniu dokumentu gwarancyjnego przez Zamawiającego, nie dopełni obowiązku naprawy lub wymiany sprzętu na wolny od wad w terminie określonym w dokumencie gwarancyjnym, Zamawiającemu przysługują roszczenia z tytułu rękojmi za wady fizyczne.

**§ 6**

**Podwykonawcy ( dotyczy*/nie dotyczy*)**

1. Wykonawca zleca pod warunkiem, że termin zakończenia przedmiotu umowy i cena umowna przedstawiona w ofercie nie ulegają zmianie, zgodnie z opisem przedmioty zamówienia i ofertą, część czynności objętych umową Podwykonawcy: a)Firmie……. z siedzibą ……. NIP ……, nr konta bankowego ……, w zakresie ……

2. Zlecenie podwykonania nie zwalnia Wykonawcy od odpowiedzialności i zobowiązań wynikających z niniejszej umowy.

3. Wykonawca nie może zaangażować do wykonania Umowy podwykonawców, którzy nie są wymienieni w niniejszej umowie, bez uprzedniej zgody Zamawiającego wyrażonej na piśmie.

4. Wykonawca gwarantuje, że podwykonawca posiada odpowiednie uprawnienia w takim zakresie, aby wykonać prawidłowo zamówienie objęte umową.

5. Wykonawca zapewnia, że podwykonawcy będą przestrzegać wszelkich postanowień umowy.

6. Wykonawca odpowiada wobec Zamawiającego za wszelkie działania lub zaniechania swoich podwykonawców jak za swoje działania lub zaniechania. Wykonawca ponosi wobec Zamawiającego pełną odpowiedzialność wraz z gwarancją za czynności, które wykonuje przy pomocy podwykonawcy, elementy umowy, w tym w szczególności zakres prac, termin wykonania oraz wynagrodzenie.

7. Wykonawca przedkłada Zamawiającemu poświadczoną za zgodność z oryginałem kopię zawartej umowy o podwykonawstwo w terminie 7 dni od dnia jej zawarcia.

8. Zamawiający dokona bezpośredniej zapłaty wynagrodzenia przysługującego podwykonawcom w przypadku, gdy Wykonawca uchyli się od obowiązku zapłaty wynagrodzenia podwykonawcom.

9. Jako uchylenie się od obowiązku zapłaty przez Wykonawcę wynagrodzenia należnego podwykonawcom uznany będzie brak przedłożenia dowodów zapłaty podwykonawcom.

10. W przypadku występowania płatności, do których uprawnieni są podwykonawcy, Wykonawca w terminie 2 dni od daty wystawienia własnej faktury lub rachunku przedłoży Zamawiającemu dowód zapłaty należności na rzecz podwykonawców z tytułu czynności objętych w fakturze lub rachunku Wykonawcy.

11. W przypadku dokonania bezpośredniej zapłaty podwykonawcy, o których mowa w ust. 10, Zamawiający potrąci kwotę wypłaconego wynagrodzenia z wynagrodzenia należnego Wykonawcy.

**§ 7.**

**Wartość umowy, zapłata ceny**

1. Wartość umowy opiewa na kwotę **…….. zł brutto** (słownie ……) w tym podatek **VAT …..%**;
2. Zapłata ceny za dostarczony sprzęt nastąpi przelewem na rachunek bankowy Wykonawcy wskazany przez niego na fakturze lub rachunku.
3. Zamawiający zobowiązuje się dokonać zapłaty należności przelewem w terminie 30 dni od daty otrzymania poprawnie wystawionej faktury, przy czym za dzień zapłaty uważa się dzień obciążenia rachunku bankowego Zamawiającego.
4. Podstawą do wystawienia faktury lub rachunku będzie protokół odbioru sprzętu objętego umową.
5. W przypadku niedotrzymania terminu płatności, o którym mowa w §7 ust. 3, przez Zamawiającego, Wykonawca może naliczyć odsetki ustawowe.
6. Wszelkie płatności będą dokonywanie w złotych polskich.

**§ 8.**

**Zmiana stron umowy**

Zmiana wierzyciela może nastąpić tylko po wyrażeniu zgody przez zamawiającego w formie pisemnej.

**§ 9.**

**Opóźnienie Wykonawcy, kary umowne i odstąpienie od umowy**

1. W przypadku opóźnienia Wykonawcy w dostarczeniu sprzętu w całości lub w części Zamawiający naliczy karę umowną, której wysokość określa się na 0,5% wartości brutto umowy za każdy dzień opóźnienia.
2. W przypadku odstąpienia od umowy z winy Wykonawcy zapłaci on Zamawiającemu karę umowną w wysokości 10% wartości brutto umowy.
3. W przypadku odstąpienia od umowy z winy Zamawiającego zapłaci on Wykonawcy karę umowną w wysokości 10% wartości brutto umowy.
4. W przypadku ujawnienia wady w zakupionym przedmiocie umowy Zamawiający wyznaczy Wykonawcy termin do wymiany towaru na wolny od wad. Z tytułu opóźnienia w dostarczeniu sprzętu wolnego od wad, Zamawiający naliczy karę umowną w wysokości 0,2% wartości brutto wadliwego przedmiotu umowy za każdy dzień opóźnienia.
5. 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 dnia powzięcia wiadomości o tych okolicznościach. W takim wypadku Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy.
6. Zamawiający zastrzega sobie prawo do odszkodowania uzupełniającego przenoszącego wysokość zastrzeżonych kar umownych do wysokości poniesionej szkody.

**§ 10.**

**Rozstrzyganie sporów**

1. Zamawiający i Wykonawca podejmą starania w celu polubownego rozstrzygnięcia wszelkich sporów powstałych między nimi a wynikających z umowy lub pozostających w pośrednim bądź bezpośrednim związku z umową, na drodze bezpośrednich negocjacji.

2. Jeśli po 30 dniach od rozpoczęcia bezpośrednich negocjacji, Zamawiający i Wykonawca nie są w stanie polubownie rozstrzygnąć sporu, to każda ze Stron może poddać spór rozstrzygnięciu sądu powszechnego, właściwego dla siedziby Zamawiającego.

**§ 11.**

**Prawo właściwe, język, zmiany umowy**

1. W zakresie nieuregulowanym w umowie znajdują zastosowanie przepisy regulujące kwestię udzielania zamówień publicznych, a w zakresie niesprzecznym z tymi przepisami – Kodeks cywilny.
2. Niniejsza umowa została zawarta w języku polskim.
3. Zakazuje się zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy, chyba, że zmiany zostały przewidziane w zapytaniu ofertowym lub opisie przedmiotu zamówienia w postaci jednoznacznych postanowień umownych, które określają ich zakres i charakter oraz warunki wprowadzenia zmian.
4. Zamawiający przewiduje możliwość zmiany umowy w przypadku zmiany stawki podatku VAT wprowadzonej przepisami prawa - może się zmienić od dnia wejścia w życie danego aktu prawnego, w takim przypadku zmieni się wartość stawki podatku VAT i ceny brutto, cena netto pozostanie bez zmian.
5. Wszelkie zmiany umowy wymagają zachowania formy pisemnej, pod rygorem nieważności.
6. Zmiany dokonane z naruszeniem ust. 3,4 i 5 niniejszego § są nieważne.

**§ 12.**

**Egzemplarze umowy**

Umowa została sporządzona w trzech jednobrzmiących egzemplarzach, z czego jeden egzemplarz dla Wykonawcy oraz dwa egzemplarze dla Zamawiającego.

Załącznik do umowy:
Załącznik nr 1 – Formularz oferty
Załącznik nr 2 - Specyfikacja techniczna
Załącznik nr 3 – protokół odbioru

Akceptuje pod względem finansowym

……

Główny Księgowy

**WYKONAWCA** **ZAMAWIAJĄCY**