

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego na:

**Dostawę laptopów z oprogramowaniem, licencji oraz akcesoriów komputerowych dla
Instytutu Agrofizyki im. B. Dobrzańskiego Polskiej Akademii Nauk w Lublinie z
podziałem na 14 części.**

W części 1 i 8 Zamówienie finansowane z środków otrzymanych od Narodowego Centrum Badań i Rozwoju na realizację projektu: „Sonda profilowa TDT do pomiaru wilgotności, temperatury i elektrycznej konduktywności gleby” (akronim: PROFILE-TDT) nr umowy STAIR/5/201

W części 2; 3; 4; 6; 7; 10; 11; 12; 13; 14 Środki własne Instytutu Agrofizyki im. B. Dobrzańskiego Polskiej Akademii Nauk

W części 1; 5; 8 i 9 Zamówienie finansowane z środków otrzymanych od Narodowego Centrum Badań i Rozwoju na realizację projektu „Mobilny system iniekcyjnego, precyzyjnego nawadniania i nawożenia, zaspokajający indywidualne potrzeby rośliny” (Akronim: MSINiN), nr umowy: BIOSTRATEG3/343547/8/NCBR/2017)

znak sprawy: A-2401-9/2019

ZATWIERDZAM

D Y R E K T O R

Stawinski

prof. dr hab. Cezary Stawiński

Lublin, dnia 28 lutego 2019 r.

Dyrektor IA PAN

SPIS ROZDZIAŁÓW:

- I. Nazwa (firma) oraz adres Zamawiającego**
- II. Tryb udzielenia zamówienia**
- III. Opis przedmiotu zamówienia**
- IV. Termin wykonania zamówienia**
- V. Warunki udziału w postępowaniu i podstawy wykluczenia**
- VI. Wykaz oświadczeń lub dokumentów, potwierdzających spełnienie warunków udziału w postępowaniu oraz brak podstaw wykluczenia**
- VII. Informacje o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń i/lub dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami**
- VIII. Wymagania dotyczące wadium**
- IX. Termin związania ofertą**
- X. Opis sposobu przygotowania oferty**
- XI. Miejsce oraz termin składania i otwarcia ofert**
- XII. Opis sposobu obliczenia ceny oferty**
- XIII. Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem wag tych kryteriów i sposobu oceny ofert**
- XIV. Informacja o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego**
- XV. Wymagania dotyczące zabezpieczenia należytego wykonania umowy**
- XVI. Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego**
- XVII. Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy w toku postępowania o udzielenie zamówienia**

I. NAZWA (FIRMA) ORAZ ADRES ZAMAWIAJĄCEGO :

**Instytut Agrofizyki im. Bohdana Dobrzańskiego
Polskiej Akademii Nauk w Lublinie
ul. Doświadczalna 4, 20–290 Lublin
Tel. (081) 744-50-61, Fax. (081) 744-50-67
NIP: 946-18-24-287 Regon: 000326380
<http://www.ipan.lublin.pl>**

Sposób i osoby uprawnione do porozumiewania się z Wykonawcami wskazano w Rozdziale VII SIWZ.

II. TRYB UDZIELENIA ZAMÓWIENIA :

1. Postępowanie będzie prowadzone w trybie przetargu nieograniczonego na podstawie art. 10 ust. 1 oraz art. 24 aa i art. 39 – 46 ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (Dz. U. z 2018 r., poz. 1986 z późn. zm.)
2. Wartość zamówienia: poniżej kwot określonych na podstawie przepisów art. 11 ust 8 Pzp.
3. W niniejszym postępowaniu Zamawiający, zgodnie z art. 24 aa ustawy pzp, zastosuje tzw. procedurę odwróconą, zgodnie z którą najpierw dokona oceny ofert pod kątem przesłanek odrzucenia oferty na podstawie art. 89 ust. 1 ustawy pzp oraz kryteriów oceny ofert opisanych w SIWZ, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu, czyli dokona oceny podmiotowej Wykonawcy badając oświadczenie wstępne, a następnie zażąda przedłożenia dokumentów w trybie art. 26 ust. 1 ustawy pzp.

III. OPIS PRZEDMIOTU ZAMÓWIENIA I OPIS CZĘŚCI ZAMÓWIENIA:

1. Przedmiotem zamówienia jest **dostawa laptopów z oprogramowaniem, licencji oraz akcesoriów komputerowych dla Instytutu Agrofizyki im. B. Dobrzańskiego Polskiej Akademii Nauk w Lublinie z podziałem na 14 części.**
2. Zakres zamówienia obejmuje dostawę do Instytutu Agrofizyki im. B. Dobrzańskiego Polskiej Akademii Nauk w Lublinie:
 - Część 1 – Dostawa komputerów PC laptopów – 9 szt., zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1.1**
 - Część 2 – Dostawa licencji na uaktualnienie systemu operacyjnego do wersji profesjonalnej (wersja edukacyjna)– 8 szt., zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1.2.**
 - Część 3 – Dostawa licencji na uaktualnienie systemu operacyjnego do wersji profesjonalnej EN (wersja edukacyjna)– 1 szt., zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1.3.**

- Część 4 – Dostawa Pakietu oprogramowania biurowego (wersja edukacyjna) – 13 szt., zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1.4.**
- Część 5 – Dostawa karty graficznej – 1 szt., zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1.5.**
- Część 6 – Dostawa dysku wewnętrznego SSD 250 GB– 2 szt., zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1.6.**
- Część 7 – Dostawa pamięci RAM 4 GB – 1 szt., zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1.7.**
- Część 8 – Dostawa karty micro SD 256 GB – 10 szt., zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1.8.**
- Część 9 – Dostawa dysku wewnętrznego 500 GB –1 szt., zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1.9.**
- Część 10 – Dostawa pakietu bezpieczeństwa antywirusowego przeznaczonego do ochrony komputerów – licencja – 250 szt., pakietu ochrony skrzynek pocztowych –licencja – 200 szt., pakietu ochrony urządzeń mobilnych – licencja – 5 szt., zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1.10.**
- Część 11 – Dostawa komputerów stacjonarnych – 4 szt., zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1.11.**
- Część 12 – Dostawa monitorów 24 cale – 5 szt., zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1.12.**
- Część 13 – Dostawa listwy głośnikowej dedykowanej do monitora – 5 szt., zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1.13.**
- Część 14 – Dostawa zestawów „klawiatura i mysz bezprzewodowa” – 7 szt., zgodnie ze szczegółowym opisem przedmiotu zamówienia stanowiącym załącznik nr 1.14.**

3. CPV:

- Część 1 – 30213100-6 Komputery przenośne,
Część 2 – 48620000-0 Systemy operacyjne
Część 3 – 48620000-0 Systemy operacyjne
Część 4 – 48310000-4 Pakiety oprogramowania do tworzenia dokumentów
Część 5 – 30237200-1 Akcesoria komputerowe
Część 6 – 30234500-3 Pamięci do przechowywania danych, 30233180-6 Urządzenia z pamięcią flash
Część 7 – 30236110-6 Pamięć o dostępie swobodnym (RAM)
Część 8 – 30233180-6 Urządzenia z pamięcią flash, 30234500-3 Pamięci do przechowywania danych
Część 9 – 30234500-3 Pamięci do przechowywania danych, 30233180-6 Urządzenia z pamięcią flash
Część 10: 48760000-3 Pakiety oprogramowania do ochrony antywirusowej,
Część 11: 30213300-8 Komputer biurkowy,

Część 12: 30231310-3 Wyświetlacze płaskie,

Część 13: 32342412-3 Głośniki,

Część 14: 30237460-1 Klawiatury komputerowe, 30237410-6 Myszka komputerowa

4. Wymagania dotyczące przedmiotu zamówienia:

- 4.1.** Zamawiający wymaga dostawy sprzętu fabrycznie nowego, nieuszkodzonego, nie regenerowanego, nie będącego uprzednio przedmiotem wystaw i prezentacji, kompletnego i gotowego do użycia po zamontowaniu (tj. bez jakichkolwiek dodatkowych zakupów i inwestycji), nieobciążonego prawami osób lub podmiotów trzecich.
- 4.2.** Przedmiot zamówienia musi być dostarczony Zamawiającemu w oryginalnych fabrycznych opakowaniach, których przechowywanie przez Zamawiającego nie jest wymagane do zachowania udzielonej gwarancji.
- 4.3.** Warunki gwarancji i serwisu nie mogą być gorsze od warunków gwarancji i serwisu producenta oferowanego sprzętu.

5. Rozwiązania równoważne:

- 1) Ilekroć w opisie przedmiotu zamówienia zawartym w SIWZ wskazane zostały normy, znaki towarowe, patenty, pochodzenie, aprobaty lub specyfikacje techniczne należy rozumieć je tylko jako przykładowe, Zamawiający dopuszcza rozwiązania (oferty) równoważne.
 - 2) Za ofertę równoważną Zamawiający uzna tę, która spełnia wszystkie wymagania Zamawiającego określone w opisie przedmiotu zamówienia zawartym w Szczegółowym opisie przedmiotu zamówienia tj. w załączniku nr od 1.1 do 1.14. do SIWZ oraz Zestawieniu wymaganych parametrów użytkowych stanowiących załącznik nr od 6.1 do 6.14 do SIWZ, których standardy, parametry techniczne i funkcjonalne są identyczne lub lepsze niż wskazane w ww. zał. do SIWZ.
 - 3) Ewentualne wskazane przez Zamawiającego nazwy, producenta mają na celu określenie klasy funkcjonalności, przeznaczenia sprzętu produktu będącego przedmiotem zamówienia i służą ustaleniu standardu nie wskazują natomiast na konkretny wyrób lub konkretnego producenta.
 - 4) Wykonawca, który powoła się na rozwiązania równoważne, jest obowiązany wykazać w sposób nie budzący wątpliwości, że oferowany przez niego przedmiot zamówienia spełnia wymagania określone przez Zamawiającego.
 - 5) W przypadku wątpliwości Zamawiającego związanych ze stwierdzeniem równoważności złożonej oferty wszelkie obowiązki związane z potwierdzeniem równoważności spoczywają na Wykonawcy.
- 6.** Wykonawca jest zobowiązany zrealizować zamówienie na zasadach i warunkach opisanych we wzorach umów stanowiącym załącznik nr 5.1; 5.2; 5.3 do SIWZ.
- 7. Wykonawca udzieli Zamawiającemu gwarancji oraz wsparcia technicznego na przedmiot zamówienia na okres:**
- **W części 1; 13 gwarancja minimum 12 miesięcy** licząc od daty podpisania protokołu zdawczo-odbiorczego przez przedstawiciela Zamawiającego i Wykonawcy.



- W części 5; 6; 7; 11; 14 gwarancja minimum 24 miesiące licząc od daty podpisania protokołu zdawczo-odbiorczego przez przedstawiciela Zamawiającego i Wykonawcy.
- W części 8; 9; 12 gwarancja minimum 36 miesięcy licząc od daty podpisania protokołu zdawczo-odbiorczego przez przedstawiciela Zamawiającego i Wykonawcy.
- W części 10 minimum 36 miesięcy wsparcia technicznego licząc od daty podpisania protokołu zdawczo-odbiorczego przez przedstawiciela Zamawiającego i Wykonawcy.
- W części 2; 3; 4 minimum 12 miesięcy wsparcia technicznego licząc od daty podpisania protokołu zdawczo-odbiorczego przez przedstawiciela Zamawiającego i Wykonawcy.

UWAGA!!!

Termin gwarancji stanowi kryterium oceny ofert w części 1; 5; 6; 7; 8; 9; 11; 12; 13; 14 zgodnie z Rozdziałem XIII SIWZ.

UWAGA!!!

Termin wsparcia technicznego stanowi kryterium oceny ofert w części 2; 3; 4; 10 zgodnie z Rozdziałem XIII SIWZ.

8. Niezależnie od uprawnień z tytułu gwarancji, Zamawiający może wykonywać uprawnienia z tytułu rękojmi na zasadach ogólnych z tym, że okres rękojmi jest równy okresowi gwarancji.
9. Zamawiający dopuszcza składanie ofert częściowych wg niżej podanego podziału:
 - Część 1 – Dostawa komputerów PC laptopów – 9 szt.,
 - Część 2 – Dostawa licencji na uaktualnienie systemu operacyjnego do wersji profesjonalnej (wersja edukacyjna)– 8 szt.,
 - Część 3 – Dostawa licencji na uaktualnienie systemu operacyjnego do wersji profesjonalnej EN (wersja edukacyjna)– 1 szt.,
 - Część 4 – Dostawa Pakietu oprogramowania biurowego (wersja edukacyjna) – 13 szt.,
 - Część 5 – Dostawa karty graficznej – 1 szt.,
 - Część 6 – Dostawa dysku wewnętrznego SSD 250 GB– 2 szt.,
 - Część 7 – Dostawa pamięci RAM 4 GB – 1 szt.,
 - Część 8 – Dostawa karty micro SD 256 GB – 10 szt.,
 - Część 9 – Dostawa dysku wewnętrznego 500 GB –1 szt.,
 - Część 10 – Dostawa pakietu bezpieczeństwa antywirusowego przeznaczonego do ochrony komputerów – licencja – 250 szt., pakietu ochrony skrzynek pocztowych – licencja – 200 szt., pakietu ochrony urządzeń mobilnych –licencja – 5 szt.,
 - Część 11 – Dostawa komputerów stacjonarnych – 4 szt.,
 - Część 12 – Dostawa monitorów 24 cale – 5 szt.,

Część 13 – Dostawa listwy głośnikowej dedykowanej do monitora – 5 szt.,

Część 14 – Dostawa zestawów „klawiatura i mysz bezprzewodowa” – 7 szt.,

10. Wykonawca może złożyć ofertę na dowolną ilość zadań (ofert częściowych).

11. Wykonawca składający ofertę na wykonanie więcej niż jednej części winien podać w ofercie warunki wykonania każdej części zamówienia oddzielnie.

12. Dodatkowe informacje dotyczące zamówienia:

- 1) Zamawiający nie przewiduje zawarcia umowy ramowej.
- 2) Zamawiający nie przewiduje zamówień, o których mowa w art. 67 ust. 1 pkt. 7 ustawy.
- 3) Zamawiający nie dopuszcza możliwości składania ofert wariantowych.
- 4) Zamawiający nie przewiduje aukcji elektronicznej.
- 5) Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
- 6) Zamawiający nie określa w opisie przedmiotu zamówienia wymagań określonych w art. 29 ust. 3 a ustawy Pzp.
- 7) Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy/om. Zamawiający żąda wskazania przez Wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez Wykonawcę firm podwykonawców – zgodnie z treścią oświadczenia, o którym mowa w Rozdziale VI lit. A pkt. 1 SIWZ. Informację w tym zakresie należy umieścić w Oświadczeniu Wykonawcy (załącznik nr 3A do SIWZ). W przypadku braku wskazania w formularzu ofertowym części zamówienia, której wykonanie będzie powierzone podwykonawcom, przyjmuje się, że całość zamówienia zostanie zrealizowana siłami własnymi Wykonawcy. Zamawiający nie zastrzega obowiązku osobistego wykonania przez wykonawcę kluczowych części zamówienia. Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się, na zasadach określonych w art. 22a ust. 1 ustawy Pzp. W celu wykazania spełnienia warunków udziału w postępowaniu, Wykonawca jest obowiązany wykazać Zamawiającemu, że proponowany inny podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż podwykonawca, na którego zasoby Wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia. Jeżeli Zamawiający stwierdzi, że wobec danego podwykonawcy zachodzą podstawy wykluczenia, Wykonawca zobowiązany będzie zastąpić tego podwykonawcę lub zrezygnować z powierzenia wykonania części zamówienia podwykonawcy. Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie zamówienia.

IV. TERMIN WYKONANIA ZAMÓWIENIA:

Zamawiający wymaga, dla części **5; 6; 8; 11; 12**; aby przedmiot zamówienia został zrealizowany w terminie maksymalnie **do 14 dni kalendarzowych licząc od daty zawarcia umowy**.

UWAGA!!!

Termin realizacji dostawy stanowi kryterium oceny ofert w części 1; 2; 3; 4; 7; 9; 10; 13; 14, zgodnie z wymaganiami określonymi w Rozdziale XIII SIWZ.

V. WARUNKI UDZIAŁU W POSTĘPOWANIU I PODSTAWY WYKLUCZENIA :

1. O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy:
 - 1.1. **nie podlegają wykluczeniu w okolicznościach, o których mowa w art. 24 ust. 1 pzp (zgodnie z Rozdziałem VI)**
 - 1.2. **spełniają warunki udziału w postępowaniu, dotyczące:**
 - 1) kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów.
Zamawiający nie określa szczegółowego sposobu oceny spełniania tego warunku.
 - 2) sytuacji ekonomicznej lub finansowej.
Zamawiający nie określa szczegółowego sposobu oceny spełniania tego warunku.
 - 3) zdolności technicznej lub zawodowej
Zamawiający nie określa szczegółowego sposobu oceny spełniania tego warunku.
2. Ocena spełniania warunków udziału w postępowaniu o zamówienie publiczne przeprowadzona będzie w oparciu o złożone przez wykonawców oświadczenia i dokumenty zgodnie z formułą „spełnia – nie spełnia”.

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 nimi stosunków prawnych.

Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, musi udowodnić zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając w tym celu **pisemne (w formie oryginału) zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.**

Dla swojej skuteczności zobowiązanie musi być złożone przez osobę/y uprawnione do reprezentowania podmiotu trzeciego w powyższym zakresie. Zobowiązanie złożone przez osobę nieuprawnioną nie dowodzi udostępnienia zasobu przez podmiot trzeci.

3. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia:
 - 3.1 brak podstaw do wykluczenia z postępowania o udzielenie zamówienia Wykonawcy w okolicznościach, o których mowa powyżej w pkt 1.1, tj. o których mowa w art. 24 ust. 1 ustawy Pzp, musi zostać wykazany przez każdego z Wykonawców.

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

A) Dokumenty i oświadczenia składane wraz z ofertą:

1. Do oferty każdy Wykonawca musi dołączyć aktualne na dzień składania ofert oświadczenie w zakresie wskazanym w **Załączniku nr 3 A i Załączniku nr 3**

B do SIWZ. Informacje zawarte w oświadczenie stanowiąc będą wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu i spełnia warunki udziału w postępowaniu.

2. Dokument (lub dokumenty), z których wynikać będzie, że osoba (osoby) podpisująca (podpisujące) ofertę jest upoważniona do reprezentowania Wykonawcy w postępowaniu i zaciągania zobowiązań w wysokości odpowiadającej cenie oferty.
3. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenia, o którym mowa w pkt 1, składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenie ma potwierdzać spełnianie warunków udziału w postępowaniu, brak podstaw do wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu, oraz brak podstaw wykluczenia.
4. Wykonawca, który zamierza powierzyć wykonanie części zamówienia podwykonawcom, w celu wykazania braku istnienia wobec nich podstaw wykluczenia z udziału w postępowaniu, zamieszcza informację o podwykonawcach w oświadczeniu, o którym mowa w pkt. 1.

B) Oświadczenie składane po otwarciu ofert, w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5 ustawy Pzp:

1. Wykonawca, w terminie **3 dni** od zamieszczenia na stronie internetowej Zamawiającego informacji, o której mowa w art. 86 ust. 5 ustawy Pzp, przekazuje Zamawiającemu **oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy Pzp (zgodnie ze wzorem stanowiącym Załącznik nr 4 do SIWZ)**; W przypadku przynależności do tej samej grupy kapitałowej, Wykonawca może złożyć wraz z oświadczeniem dokumenty bądź informacje potwierdzające, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu (w formie oryginału)

C) Informacje dotyczące procedury oraz formy dokumentów:

1. W niniejszym postępowaniu Zamawiający, **zgodnie z art. 24 aa ustawy pzp**, zastosuje tzw. **procedurę odwróconą**, zgodnie z którą najpierw dokona oceny ofert pod kątem przesłanek odrzucenia oferty na podstawie art. 89 ust. 1 ustawy pzp oraz kryteriów oceny ofert opisanych w SIWZ, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu, czyli dokona oceny podmiotowej Wykonawcy badając oświadczenie wstępne, a następnie zażąda przedłożenia dokumentów w trybie art. 26 ust. 2 ustawy pzp.
2. Jeżeli Wykonawca nie złoży oświadczenia, o którym mowa w Rozdziale VI lit. A, 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 będą wskazane przez Zamawiającego wątpliwości, Zamawiający wezwie do ich

złożenia, uzupełnienia, poprawienia w terminie przez siebie wskazanym, chyba że mimo ich złożenia oferta Wykonawcy podlegałaby odrzuceniu albo konieczne byłoby unieważnienie postępowania.

3. Jeżeli Wykonawca nie złożył wymaganych pełnomocnictw albo złożył wadliwe pełnomocnictwa, Zamawiający wezwie do ich złożenia w terminie przez siebie wskazanym, chyba że mimo ich złożenia oferta Wykonawcy podlegałaby odrzuceniu albo konieczne byłoby unieważnienie postępowania.
4. Oświadczenia, o których mowa w Rozporządzeniu Ministra Rozwoju z dnia 26 lipca 2016 roku w sprawie rodzajów dokumentów, jakich może żądać Zamawiający od Wykonawcy w postępowaniu o udzielenie zamówienia publicznego (Dz. U z 2016 r., poz. 1126), dotyczące Wykonawcy i innych podmiotów, na których zdolnościach lub sytuacji polega Wykonawca na zasadach określonych w art. 22 a ustawy oraz dotyczące podwykonawców, składane są w oryginale.
5. Dokumenty, o których mowa w Rozporządzeniu, inne niż oświadczenia, o których mowa w pkt. 10, składane są w oryginale lub kopii poświadczonej za zgodność z oryginałem.
6. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego lub podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą.
7. Poświadczenie za zgodność z oryginałem musi nastąpić w formie pisemnej.
8. Gdy przedstawiona kopia dokumentu będzie nieczytelna lub będzie budziła wątpliwość, co do jej prawdziwości, Zamawiający może zażądać przedstawienia oryginału lub notarialnie poświadczonej kopii dokumentów, o których mowa w Rozporządzeniu, innych niż oświadczenia.
9. Dokumenty sporządzone w języku obcym należy złożyć wraz z tłumaczeniem na język polski.
10. W zakresie nieuregulowanym w SIWZ, zastosowanie mają przepisy Rozporządzenia Ministra Rozwoju z dnia 26 lipca 2016 roku w sprawie rodzajów dokumentów, jakich może żądać Zamawiający od Wykonawcy w postępowaniu o udzielenie zamówienia publicznego (Dz. U z 2016 r., poz. 1126)
11. W przypadku wskazania przez Wykonawcę w oświadczeniu według Załącznika nr 3 A przez Wykonawcę dostępności oświadczeń lub dokumentów składanych w celu potwierdzenia spełnienia warunków udziału w postępowaniu lub braku podstaw wykluczenia, w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych, Zamawiający pobierze samodzielnie z tych baz danych wskazane przez Wykonawcę oświadczenia lub dokumenty.
12. W przypadku wskazania przez Wykonawcę w oświadczeniu według Załącznika nr 3 A dostępności oświadczeń lub dokumentów składanych w celu potwierdzenia spełnienia

warunków udziału w postępowaniu lub braku podstaw wykluczenia, które znajdują się w posiadaniu Zamawiającego, w szczególności oświadczeń lub dokumentów przechowywanych przez Zamawiającego zgodnie z art. 97 ust. 1 ustawy Pzp, Zamawiający w celu potwierdzenia okoliczności, o których mowa w art. 25 ust. 1 pkt 1 i 3 ustawy Pzp, skorzysta z posiadanych oświadczeń lub dokumentów, o ile będą one aktualne.

13. Zamawiający może zażądać od Wykonawcy przedstawienia tłumaczenia na język polski wskazanych przez Wykonawcę i pobranych samodzielnie przez Zamawiającego oświadczeń i dokumentów, o których mowa w pkt. 11 i 12.

D) Informacje dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych :

Zgodnie z art. 13 ust. 1 i 2 oraz art. 14 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), dalej RODO, informuję, że:

1. Administratorem danych osobowych przetwarzanych w w/w celach jest Instytut Agrofizyki im. Bohdana Dobrzańskiego Polskiej Akademii Nauk, ul. Doświadczalna 4, 20-290 Lublin, www.ipan.lublin.pl
2. Instytut – jako administrator danych - doloży wszelkich starań, aby w jak najpełniejszym stopniu zrealizować wymogi Rozporządzenia i w ten sposób chronić Pani/Pana dane osobowe.
3. Nadzór nad prawidłowym przetwarzaniem danych osobowych w Instytucie sprawuje Inspektor Ochrony Danych, z którym można się kontaktować pod adresem e-mail: k.kajdrowicz@ipan.lublin.pl Dodatkowe dane osobowe Inspektora są dostępne na www.ipan.lublin.pl.
4. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym postępowaniem o udzielenie zamówienia publicznego, a po zawarciu umowy również na podstawie art. 6 ust. 1 lit.b) RODO.
5. 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”;
6. 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, nie krótszy jednak niż cały czas trwania umowy
7. 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;
8. w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
9. 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 (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);
- 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 ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego);
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy 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.

VII. INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ I DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI:

1. Zasady i formy przekazywania oświadczeń, wniosków i innych dokumentów:

- 1) Oferty w przedmiotowym postępowaniu o udzielenie zamówienia publicznego składa się pod rygorem nieważności w formie pisemnej, w języku polskim.
- 2) Komunikacja pomiędzy Zamawiającym a Wykonawcami w przedmiotowym postępowaniu odbywać się będzie poprzez składanie/wymianę korespondencji: za pośrednictwem operatora pocztowego w rozumieniu ustawy z dnia 23 listopada 2012 roku Prawo pocztowe (Dz. U. 2012 r., poz. 1529 oraz 2015 r., poz. 1830 z późn. zm), lub osobiście, lub za pośrednictwem pośłańca, lub faksu, lub e-mailem.
- 3) Korespondencję, tj. wszelkie zawiadomienia, oświadczenia, wnioski oraz informacje Zamawiający oraz Wykonawcy mogą przekazywać pisemnie, faksem lub drogą



elektroniczną, za wyjątkiem oferty, umowy oraz oświadczeń i dokumentów wymienionych w Rozdziale VI niniejszej SIWZ (również w przypadku ich złożenia w wyniku wezwania przez Zamawiającego, dla których przepisy prawa przewidują wyłącznie formę pisemną).

- 4) Zawiadomienia, oświadczenia, wnioski oraz informacje przekazywane przez Wykonawcę pisemnie powinny być składane na adres Zamawiającego. W korespondencji Wykonawca powinien posługiwać się numerem sprawy nadanej postępowaniu, który jest podany w SIWZ.
- 5) Jeżeli Zamawiający lub Wykonawca przekazują zawiadomienia, oświadczenia, wnioski oraz informacje za pośrednictwem faksu lub e-maila, każda ze stron na żądanie drugiej strony niezwłocznie potwierdza fakt ich otrzymania;
- 6) W przypadku przekazania dokumentów czy informacji przez Zamawiającego faksem na nr podany przez Wykonawcę, potwierdzenie wysłania faksem zawierające komunikat „ok” uważa się za doręczone prawidłowo.
- 7) Specyfikację Istotnych Warunków Zamówienia wraz z załącznikami można pobrać ze strony internetowej Instytutu Agrofizyki im. Bohdana Dobrzańskiego, www.ipan.lublin.pl lub uzyskać w siedzibie Zamawiającego: Instytut Agrofizyki im. Bohdana Dobrzańskiego Polskiej Akademii Nauk w Lublinie, ul. Doświadczalna 4, bud. A, pok. Nr 9.
- 8) Na stronie internetowej www.ipan.lublin.pl (zakładka „Zamówienia publiczne” - <http://bip.ipan.lublin.pl/index.php/bip?id=1>) Zamawiający będzie zamieszczał informacje wymagane ustawą Prawo zamówień publicznych związane z niniejszym postępowaniem.

2. Wyjaśnienia dotyczące treści specyfikacji istotnych warunków zamówienia:

- 1) Każdy Wykonawca ma prawo zwrócić się do Zamawiającego o wyjaśnienie treści Specyfikacji Istotnych Warunków Zamówienia.
- 2) Oświadczenia, wnioski, zawiadomienia, inne informacje oraz pytania kierowane do Zamawiającego przekazywane pisemnie należy kierować na adres Zamawiającego podany w Rozdziale I niniejszej specyfikacji. W przypadku porozumiewania się e-mailem, wszelkie zawiadomienia, oświadczenia, wnioski oraz informacje powinny być kierowane na adres: j.muszynska-sadlo@ipan.lublin.pl.
- 3) Zamawiający udzieli wyjaśnień dotyczących treści specyfikacji istotnych warunków zamówienia niezwłocznie, jednak nie później niż na **2 dni** przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści Specyfikacji Istotnych Warunków Zamówienia wpłynie do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.
- 4) Jeżeli wniosek o wyjaśnienie treści specyfikacji istotnych warunków zamówienia wpłynął po upływie terminu składania wniosku, o którym mowa w pkt 3) lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.
- 5) Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku, o którym mowa w pkt 3).



- 6) Treść zapytań wraz z wyjaśnieniami Zamawiający przekazuje wykonawcom, którym przekazał SIWZ bez ujawniania źródła zapytania oraz zamieszcza na stronie internetowej.
- 7) W uzasadnionych przypadkach Zamawiający może przed upływem terminu do składania ofert zmienić treść SIWZ. Dokonaną w ten sposób zmianę treści SIWZ udostępnia na stronie internetowej.
- 8) W przypadku rozbieżności pomiędzy treścią SIWZ, a treścią udzielonych odpowiedzi, jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie.
- 9) W związku z wynikającą z ustawy koniecznością zamieszczania treści zapytań do SIWZ, a także treści odwołań dotyczących treści ogłoszenia o zamówieniu lub postanowień SIWZ na stronie internetowej Zamawiającego, jak również ze względu na często słabą czytelność pism przysyłanych do Zamawiającego faksem i związanych z tym trudnościami skanowania, treść zapytań do niniejszej SIWZ, a także treść ewentualnego odwołania prosimy przesłać również w wersji elektronicznej pocztą e-mail na adres: j.muszynska-sadlo@ipan.lublin.pl
- 10) Zamawiający nie przewiduje zorganizowania zebrania z Wykonawcami.

3. Osoby uprawnione do porozumiewania się z Wykonawcami:

Justyna Muszyńska-Sadło

fax /81/ 744 50 67 lub

e-mail: j.muszynska-sadlo@ipan.lublin.pl

VIII. WYMAGANIA DOTYCZĄCE WADIUM.

Zamawiający nie wymaga wniesienia wadium.

IX. TERMIN ZWIĄZANIA OFERTĄ.

1. Wykonawca jest związany ofertą przez okres **30 dni** od terminu składania ofert. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
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 ofertą, zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.

X. OPIS SPOSOBU PRZYGOTOWANIA OFERTY.

1. Oferta musi zawierać następujące oświadczenia i dokumenty:

a) prawidłowo wypełniony formularz ofertowy sporządzony wg wzoru stanowiącego załącznik nr 2 do SIWZ, zawierający w szczególności: wskazanie oferowanego przedmiotu zamówienia, ceny jednostkowe oferowanych produktów, łączną ceną ofertową brutto osobno w odniesieniu do każdego zadania, zobowiązanie dotyczące terminu realizacji zamówienia, okresu gwarancji i warunków płatności, oświadczenie o okresie związania ofertą oraz o akceptacji wszystkich postanowień SIWZ i wzoru umowy bez zastrzeżeń,

- b) prawidłowo wypełniony Zestawienie wymaganych parametrów technicznych i użytkowych dla zadania na które jest składana oferta (sporządzony wg wzoru określonego odpowiednio w załączniku nr od 6.1 do 6.14 do SIWZ) zawierający w szczególności: oferowany przedmiot zamówienia (wskazanie konkretnych oferowanych produktów),
- c) dokumenty i oświadczenia wymagane do złożenia wraz z ofertą określone w Rozdziale VI lit. A SIWZ
- d) stosowne pełnomocnictwo (a) – wystawione w oryginale lub kopii poświadczonej notarialnie dla osoby (osób) podpisującej ofertę oraz poświadczającej kopie dokumentów za zgodność z oryginałem – w przypadku, gdy upoważnienie do tych czynności nie wynika bezpośrednio ze złożonego w ofercie odpisu z właściwego rejestru albo wpisu do Centralnej Ewidencji Informacji o Działalności Gospodarczej Rzeczypospolitej Polskiej. Pełnomocnictwo powinno zawierać upoważnienie do udzielania dalszych [pełnomocnictw w przypadku podpisania oferty przez pełnomocnika substytucyjnego, w takim wypadku do oferty należy także załączyć pełnomocnictwo substytucyjne,
- e) w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia (na zasadach konsorcjum), dokument ustanawiający pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
- Oferta musi być napisana w języku polskim, na maszynie do pisania, komputerze lub inną trwałą i czytelną techniką oraz podpisana przez osobę lub osoby upoważnione do podejmowania zobowiązań w imieniu Wykonawcy zgodnie z wpisem o reprezentacji w stosownym dokumencie uprawniającym do występowania w obrocie prawnym lub udzielonym pełnomocnictwem. Osoba/y podpisujące ofertę muszą być upoważnione do reprezentowania Wykonawcy na zewnątrz i zaciągania zobowiązań w wysokości odpowiadającej cenie oferty.
 - W przypadku podpisania oferty oraz poświadczenia za zgodność z oryginałem kopii dokumentów przez osobę nie wymienioną w dokumencie rejestracyjnych (ewidencyjnym) Wykonawcy, osoba ta powinna posiadać stosowne pełnomocnictwo wystawione w oryginale lub kopii poświadczonej notarialnie. Z pełnomocnictwa musi jednoznacznie wynikać do jakich czynności prawnych dana osoba/y została/y umocowana/e (w formie oryginału lub kopii poświadczonej za zgodność z oryginałem)
 - Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
 - Wykonawca ma prawo złożyć tylko jedną ofertę, zawierającą jedną, jednoznacznie opisaną propozycję. Złożenie większej liczby ofert spowoduje odrzucenie wszystkich ofert złożonych przez danego Wykonawcę.
 - Treść oferty musi odpowiadać treści SIWZ. Zamawiający nie wyraża zgody na złożenie oferty w formie elektronicznej.
 - Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.



8. Zaleca się, aby wszystkie strony oferty były zszyte w sposób trwały, zapobiegający możliwości dekompletacji zawartości oferty (np. zbindowana, zszyta uniemożliwiającej jej samodzielną dekompletację) oraz aby wszystkie, zapisane strony oferty wraz z załącznikami były ponumerowane.
9. Poprawki lub zmiany w ofercie muszą być naniesione czytelnie oraz opatrzone podpisem osoby podpisującej ofertę.
10. Ofertę należy złożyć w zamkniętej kopercie. Całość oferty powinna być złożona w formie uniemożliwiającej jej przypadkowe zdekompletowanie.
11. Wykonawca powinien umieścić ofertę w zewnętrznej i wewnętrznej kopercie z tym, że:
 1. zewnętrzna koperta powinna być zaadresowana na Zamawiającego i zawierać oznaczenie:
oferta na: **„Dostawę laptopów z oprogramowaniem, licencji oraz akcesoriów komputerowych dla Instytutu Agrofizyki im. B. Dobrzańskiego Polskiej Akademii Nauk w Lublinie z podziałem na 14 części A-2401-9/2019”** – bez nazwy i pieczętki wykonawcy;
 2. koperta wewnętrzna powinna zawierać ofertę i być zaadresowana na wykonawcę, tak aby można było odesłać ofertę w przypadku jej wycofania lub wpłynięcia po terminie.
12. Zamawiający informuje, że zgodnie z art. 8 w zw. z art. 96 ust. 3 ustawy Pzp oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r., Nr 153, poz. 1503 z późn. zm.), jeśli Wykonawca w terminie składania ofert zastrzegł, że nie mogą być one udostępniane i jednocześnie wykazał, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
13. Zamawiający zaleca, aby informacje zastrzeżone, jako tajemnica przedsiębiorstwa były przez Wykonawcę złożone w oddzielnej wewnętrznej kopercie z oznakowaniem „tajemnica przedsiębiorstwa”, lub spięte (zszyte) oddzielnie od pozostałych, jawnych elementów oferty. Brak jednoznacznego wskazania, które informacje stanowią tajemnicę przedsiębiorstwa oznaczać będzie, że wszelkie oświadczenia i zaświadczenia składane w trakcie niniejszego postępowania są jawne bez zastrzeżeń.
14. Zastrzeżenie informacji, które nie stanowią tajemnicy przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r., Nr 153, poz. 1503 z późn. zm.) będzie traktowane, jako bezskuteczne i skutkować będzie ich odtajnieniem.
15. Zamawiający informuje, że w przypadku kiedy Wykonawca otrzyma od niego wezwanie w trybie art. 90 ustawy Pzp, a złożone przez niego wyjaśnienia i/lub dowody stanowią tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r., Nr 153, poz. 1503 z późn. zm.) Wykonawcy będzie przysługiwało prawo zastrzeżenia ich jako tajemnica przedsiębiorstwa. Przedmiotowe zastrzeżenie zamawiający uzna za skuteczne wyłącznie w sytuacji, kiedy Wykonawca oprócz samego zastrzeżenia, jednocześnie wykaże, iż dane informacje stanowią tajemnicę przedsiębiorstwa.



16. Wykonawca może, przed upływem terminu do składania ofert zmienić, poprawić, modyfikować, uzupełniać lub wycofać ofertę. Powiadomienie o zamiarze wprowadzenia zmian, poprawek, modyfikacji, uzupełnień lub wycofaniu oferty należy przygotować i oznaczyć zgodnie z postanowieniami Rozdziału X pkt 11), a zewnętrzną kopertę dodatkowo oznaczyć napisem " ZMIANA" lub " WYCOFANIE".
17. Koperty oznaczone „ZMIANA” zostaną otwarte przy otwieraniu oferty Wykonawcy, który wprowadził zmiany i po stwierdzeniu poprawności procedury dokonywania zmian, zostaną dołączone do oferty.
18. Wykonawca ma prawo przed terminem składania ofert wycofać się z postępowania poprzez złożenie pisemnego powiadomienia, według tych samych zasad jak wprowadzanie zmian i poprawek z napisem na kopercie „WYCOFANIE”. Koperty oznakowane w ten sposób nie będą otwierane.
19. Wartości pieniężne wskazane w dokumentach złożonych w celu wykazania przez Wykonawcę spełniania warunków udziału w postępowaniu, o którym mowa powyżej, podane w walutach obcych, Wykonawca przeliczy na złote polskie wg średniego kursu walut NBP z dnia opublikowania ogłoszenia o niniejszym postępowaniu w Biuletynie Zamówień Publicznych.
20. Oferta, której treść nie będzie odpowiadać treści SIWZ, z zastrzeżeniem art. 87 ust. 2 pkt 3 ustawy Pzp zostanie odrzucona (art. 89 ust. 1 pkt 2 ustawy Pzp). Wszelkie niejasności i wątpliwości dotyczące treści zapisów w SIWZ należy wyjaśnić z Zamawiającym przed terminem składania ofert w trybie przewidzianym w Rozdziale VII SIWZ. Przepisy ustawy Pzp nie przewidują negocjacji warunków udzielenia zamówienia, w tym zapisów projektu umowy, po terminie otwarcia ofert.
21. Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełnienia, w zakresie, w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu zamieszcza informacje o tych podmiotach w oświadczeniach, według wzoru stanowiącego Załącznik 3 A do SIWZ.
22. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców:
 - 1) Każdy z Wykonawców wspólnie ubiegających się o zamówienie składa oświadczenia, w celu potwierdzenia spełniania warunków udziału w postępowaniu oraz brak podstaw do wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia oraz pełnomocnictwo, o którym mowa w ust. 3.
 - 2) Formularz ofertowy, o którym mowa w pkt 1 lit. a) składany przez pełnomocnika Wykonawców wspólnie ubiegających się o udzielenia zamówienia.
 - 3) Poza dokumentami wymienionymi w pkt 1 i 2 Wykonawcy wspólnie ubiegający się o udzielenie zamówienia powinni załączyć do oferty oryginał pełnomocnictwa celem ustalenia:
 - a) Wykonawcy – pełnomocnika uprawnionego do występowania w imieniu grupy Wykonawców,



b) Wykonawców ubiegających się wspólnie o przedmiotowe zamówienie publiczne (wymienionych z nazwy wraz z określeniem adresu siedziby)

Wykonawcy zobowiązani są do ustanowienia pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarciu umowy w sprawie zamówienia publicznego. Treść pełnomocnictwa powinna dokładnie określać zakres umocowania. Dokument pełnomocnictwa powinien zostać podpisany przez wszystkich Wykonawców ubiegających się wspólnie o udzielenie zamówienia, w tym Wykonawcę pełnomocnika. Podpisy muszą być złożone przez osoby uprawnione do składania oświadczeń woli. Wszelka korespondencja oraz rozliczenia dokonywane będą wyłącznie z pełnomocnikiem. Oferta musi być podpisana w taki sposób, aby prawnie zobowiązywała wszystkich Wykonawców występujących wspólnie. Zapisy dotyczące uwag odnośnie formy składanych dokumentów wymaganych od Wykonawcy mającego siedzibę lub miejsce zamieszkania za granicą stosuje się odpowiednio.

23. Dokumenty powinny być sporządzone ściśle z zaleceniami oraz przedstawionymi przez Zamawiającego wzorcami – załącznikami, a w szczególności zawierać wszystkie informacje oraz dane.
24. Właściwym i obowiązującym prawem do stosowania przy przeprowadzaniu przedmiotowego postępowania jest prawo polskie.
25. W przypadku złożenia oferty w innym miejscu niż wyznaczone lub braku odpowiedniego oznakowania koperty, czy nieprawidłowego zaadresowania koperty, Zamawiający nie ponosi odpowiedzialności za zdarzenia wynikające z powyższych działań Wykonawcy, np. przypadkowe otwarcie oferty przed wyznaczonym terminem składania ofert, jej nie otwarcie w trakcie publicznego otwarcia ofert lub złe skierowanie przesyłki.

XI. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT:

1) Miejsce składania ofert.

Ofertę Wykonawca składa (sporządzoną w formie pisemnej, w języku polskim) za pośrednictwem operatora pocztowego w rozumieniu ustawy z dnia 23 listopada 2012 r. Prawo pocztowe, osobiście lub za pośrednictwem posłańca na adres siedziby Zamawiającego - **Instytut Agrofizyki im. Bohdana Dobrzańskiego Polskiej Akademii Nauk w Lublinie, ul. Doświadczalna 4, bud. A, pok. 18 (sekretariat).**

2) Termin składania ofert.

1. Termin składania ofert upływa **w dniu 8 marca 2019 r. o godz. 12:00.**
2. Za termin złożenia oferty uważa się termin jej dotarcia do Zamawiającego.
3. Decydująca jest data i godzina wpływu oferty do siedziby Zamawiającego potwierdzona pieczęcią Zamawiającego.
4. Za prawidłowe zaadresowanie i złożenie (dostarczenie oferty w terminie i we właściwe miejsce) odpowiada Wykonawca. Zamawiający nie ponosi konsekwencji dostarczenia oferty w inne miejsce niż wymienione w pkt 1.1 lub po terminie.



5. Zamawiający niezwłocznie zawiadomi wykonawcę o złożeniu oferty po terminie oraz zwróci ofertę po upływie terminu do wniesienia odwołania, zgodnie z art. 84 ust. 2 ustawy Pzp.

3) Otwarcie ofert.

1. Z zawartością wniosków o dopuszczenie do udziału w postępowaniu lub ofert nie można zapoznać się przed upływem terminu, odpowiednio do ich złożenia lub otwarcia.
2. Otwarcie ofert jest jawne i odbędzie się **w dniu 8 marca 2019 r. o godz. 12:15** w siedzibie Instytutu Agrofizyki im. Bohdana Dobrzańskiego Polskiej Akademii Nauk w Lublinie, ul. Doświadczalna 4, pok. Nr 6 (sala seminaryjna).
3. Bezpośrednio przed otwarciem ofert Zamawiający podaje kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
4. Podczas otwarcia ofert podaje się:
 - a) nazwy (firmy) oraz adresy wykonawców, którego oferta jest otwierana,
 - b) informacje dotyczące ceny,
 - c) informacje dotyczące terminu wykonania zamówienia,
 - d) informacje dotyczące okresu gwarancji,
 - e) informacje dotyczące warunków płatności.
5. Koperty oznakowane dopiskiem „ZMIANA” zostaną otwarte przy otwieraniu oferty Wykonawcy, który wprowadził zmiany i po stwierdzeniu poprawności procedury dokonywania zmian, zostaną dołączone do oferty i zostaną otwarte przed otwarciem koperty zawierającej ofertę, której dotyczą zmiany.
6. Niezwłocznie po otwarciu ofert zamawiający zamieszcza na stronie internetowej informacje dotyczące:
 - 1) kwoty, jaką zamierza przeznaczyć na sfinansowanie zamówienia;
 - 2) firm oraz adresów wykonawców, którzy złożyli oferty w terminie;
 - 3) ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.
7. Wykonawca, w terminie 3 dni od dnia przekazania informacji, o których mowa w pkt. 5, przekazuje Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy (w formie oryginału) według wzoru zamieszczonego na stronie internetowej Zamawiającego wraz z informacją określoną w pkt. 5. Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.
8. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, każdy z Wykonawców wspólnie ubiegających się o zamówienie składa oświadczenie, o którym mowa w pkt. 6.

XII. OPIS SPOSOBU OBLICZENIA CENY OFERTY.

- 1) Rozliczenia między Zamawiającym a wykonawcą będą dokonywane w polskich złotych (PLN). Zamawiający nie przewiduje rozliczeń w walutach obcych.
- 2) Ceną podlegającą ocenie, w zakresie poszczególnych zadań, jest cena oferty brutto, inaczej zwana ceną ofertową.
- 3) Przez cenę należy rozumieć wartość wyrażoną w jednostkach pieniężnych, którą Zamawiający jest obowiązany zapłacić Wykonawcy za towar lub usługę; w cenie uwzględnia się podatek od towarów i usług oraz podatek akcyzowy, jeżeli na podstawie odrębnych przepisów sprzedaż towaru (dostawy) podlega temu obciążeniu.
- 4) Ceną ofertową ma być cena za zrealizowanie przedmiotu zamówienia zgodnie z jego opisem zawartym w opisie przedmiotu zamówienia zawartym w Szczegółowym opisie przedmiotu zamówienia tj. w załączniku nr od 1.1 do 1.14 do SIWZ, a także we wzorach umów stanowiącym załącznik nr 5.1; 5.2; 5.3 do SIWZ. Cena oferty uwzględniać ma nie tylko wartość samej dostawy przedmiotu zamówienia, podatek od towarów i usług, ale również wszystkie inne składniki wynikające z należytej realizacji przedmiotu umowy, w tym w szczególności transport, opakowanie, ubezpieczenie towaru, opusty, rabaty, dojazd pracowników firmy w celu zainstalowania i uruchomienia przedmiotu zamówienia, przeszkolenia pracowników Zamawiającego, świadczenie usług serwisowych, udzielenie licencji do oprogramowania oraz wszelkie inne koszty, konieczne dla zrealizowania przedmiotu zamówienia zgodnie z jego opisem i postanowieniami wzoru umowy.
- 5) Cena, o której mowa w pkt 3), jest ostateczną ceną, jaką Zamawiający zapłaci za zrealizowanie przedmiotu zamówienia na warunkach określonych we wzorze umowy. Każdy z Wykonawców może zaproponować tylko jedną cenę ofertową i nie może jej zmienić. Zamawiający wymaga, aby ceny jednostkowe przedstawione przez Wykonawcę w ofercie, podane były wyłącznie w wartościach dodatnich. Podanie przez Wykonawcę wartości 0 zł i mniejszej skutkować będzie odrzuceniem oferty.
- 6) Cenę ofertową dla każdej części zamówienia osobno, należy podać cyfrowo i słownie w polskiej walucie (PLN) na formularzu oferty stanowiącym załącznik nr 2 do niniejszej SIWZ. Wykonawca podaje cenę ofertową netto i brutto (z podatkiem VAT).
- 7) Cena ma być podana z dokładnością do dwóch miejsc po przecinku. Wszelkie obliczenia należy dokonać z dokładnością do pełnych groszy (z dokładnością do dwóch miejsc po przecinku, zarówno przy kwotach netto, VAT i brutto), przy czym końcówki poniżej 0,5 grosza pomija się, a końcówki 0,5 grosza i wyższe zaokrągla się w górę.
- 8) Prawidłowe ustalenie stawki podatku VAT leży po stronie Wykonawcy. Zamawiający wymaga, aby Wykonawca obliczając cenę oferty stosował stawki VAT zgodnie ze stanem prawnym obowiązującym na dzień składania ofert.
- 9) Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług w zakresie dotyczącym wewnątrzwspólnotowego nabycia towarów, Zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z obowiązującymi przepisami. Wykonawca, składając ofertę, informuje Zamawiającego, czy wybór oferty będzie

prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.

W przypadku, gdy w którejkolwiek z pozycji wskazanej w tabelach od 1 do 4 formularza ofertowego obowiązek podatkowy, zgodnie z przepisami o podatku od towarów i usług leży po stronie Zamawiającego, Wykonawca nie wypełnia w tabelach w tych pozycjach kolumn G, H oraz I. Jednocześnie w formularzu oferty oświadcza, że w tej/tych pozycji/ach obowiązek podatkowy, zgodnie z przepisami o podatku od towaru i usług, leży po stronie Zamawiającego. W takiej sytuacji Zamawiający w celu oceny złożonej oferty, do sumy wartości brutto (kol. I wiersz 2 tabeli nr 1 oraz nr 2), doda wartość netto tej/yh pozycji (kol. F) powiększoną o podatek od towarów i usług, który będzie miał obowiązek rozliczyć - podstawa prawna art. 17 ust. 1 pkt 7 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług.

Powyższy sposób wypełnienia Formularza cenowego, zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług, dotyczy takich okoliczności jak:

- wewnątrzwspólnotowe nabycie towarów,
- import usług lub towarów,
- mechanizm odwróconego obciążenia podatkiem VAT.

XIII. OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT.

1. Do wyboru najkorzystniejszej oferty Zamawiający posługiwał się będzie kryteriami cenowymi, terminem dostawy oraz kryteriami jakościowymi.
2. Zostanie wybrana oferta, która uzyska największą liczbę punktów, zgodnie z poniższymi kryteriami:

a) Kryterium cenowe (dla wszystkich części jednakowe):

1) Oferowana cena – maksymalnie 60 punktów.

W powyższym kryterium oceniana będzie łączna cena brutto oferty. Maksymalną ilość punktów w tym kryterium otrzyma wykonawca, który zaproponuje najniższą cenę, pozostali będą oceniani wg następującego wzoru:

Cena brutto oferty najniższej spośród
wszystkich ofert podlegających ocenie

Liczba punktów za kryterium cenowe $LP_c = \frac{\text{Cena brutto oferty najniższej spośród wszystkich ofert podlegających ocenie}}{\text{Cena brutto oferty badanej (ocenianej)}} \times 60 \text{ pkt}$

2) Każdy wykonawca będzie oceniany w ww. kryterium w skali od 0 do 60 punktów.

3) Zamawiający nie dopuszcza rozliczeń w walutach obcych. Rozliczenia mogą być prowadzone tylko w walucie polskiej PLN.

4) Każda część zamówienia będzie oceniana oddzielnie.

Pozostałe kryteria w odniesieniu do każdej części:

CZEŚĆ 1; 13

Waga kryterium	Opis kryterium oceny ofert
<p>b) Termin gwarancji 20%</p>	<p><u>Termin gwarancji – 20%:</u> Punkty w tym kryterium zostaną przyznane w następujący sposób:</p> <ul style="list-style-type: none"> • <u>zaoferowanie rozszerzenia gwarancji z 12 miesięcy na 24 miesiące producenta -20 pkt</u> • <u>niezaoferowanie rozszerzenia gwarancji z 12 miesięcy na 24 miesiące producenta - 0 pkt</u> <p>UWAGA!!!! Zamawiający informuje, że kryterium ma charakter zero/jedynkowy, tzn. jeżeli Wykonawca oświadczy w złożonej ofercie, że oferuje „rozszerzenie gwarancji z 12 miesięcy na 24 miesiące”, wówczas Zamawiający przyzna 20 pkt. Brak wskazania/wpisania w Formularzu oferty powyższego kryterium, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca jego nie oferuje, więc nie otrzyma punktów w tym kryterium. Zaoferowanie kryterium terminu gwarancji niezgodnego z wytycznymi Zamawiającego będzie skutkowało odrzuceniem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p>
<p>c) Termin dostawy 20%</p>	<p>Kryterium „Termin dostawy” – maksymalnie 20 punktów Zamawiający wymaga, aby przedmiot zamówienia został zrealizowany w terminie maksymalnie do 14 dni kalendarzowych licząc od daty zawarcia umowy (dotyczy wszystkich części) W powyższym kryterium oceniana będzie łączna długość terminu dostawy od dnia podpisania umowy. Zamawiający odniesie wartości z poszczególnych ofert do minimalnego oczekiwanego przez Zamawiającego terminu dostawy, Min.7 dni, natomiast nie może być on dłuższy niż 14 dni.</p> $TD = (14 \text{ dni} - Tob) : 7 \text{ dni} \times 20 \text{ pkt}$ <p>gdzie: TD – przyznane punkty; Tob – termin oferty badanej (wyrażony w dniach).</p> <p>2) Każdy wykonawca będzie oceniany w kryterium „termin dostawy” w skali od 0 do 20 punktów</p> <p>UWAGA!!!</p> <ul style="list-style-type: none"> • Zamawiający informuje, że w przypadku określenia przez Wykonawcę terminu dostawy krótszego niż 7 dni, Zamawiający przyjmie do obliczeń w kryterium oceny ofert „Termin dostawy” wartość 7 dni, natomiast termin wskazany przez Wykonawcę będzie wiążący do realizacji przez Niego zamówienia. • W przypadku określenia przez Wykonawcę terminu dostawy dłuższego niż 14 dni, oferta będzie odrzucona, jako niezgodna z SIWZ. • Termin dostawy będzie liczony od dnia zawarcia umowy.

	<p>Brak wskazania/wpisania w Formularzu oferty terminu dostawy, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca oferuje najdłuższy (maksymalny akceptowany przez Zamawiającego) termin dostawy, czyli 14 dni</p> <p>Zaoferowanie terminu realizacji niezgodnego z wytycznymi Zamawiającego będzie skutkowało odrzuceniem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p> <p>Wykonawca zobowiązany jest w ofercie wyrazić oferowany termin realizacji w dniach. W przypadku podania terminu realizacji w innej postaci Zamawiający dokona stosownych przeliczeń opierając się na postanowieniach Kodeksu cywilnego dotyczących tygodnia, miesiąca.</p> <p>Wykonawca w oferowanym terminie realizacji zamówienia musi uwzględnić wszelkie ryzyka jakie mógł przewidzieć doświadczony Wykonawca, a w szczególności ryzyka związane z realizacją przedmiotu zamówienia.</p>
--	--

Łączna liczba punktów za kryterium cenowe, termin gwarancji oraz kryterium termin dostawy będzie wzorem:

$$LP = LP_c + LP_g + LP_{td}$$

gdzie:

- LP to liczba punktów
 LP_c to kryterium cenowe
 LP_g to termin gwarancji
 LP_{td} to kryterium termin dostawy

CZĘŚĆ 2; 3; 4

Waga kryterium	Opis kryterium oceny ofert
b) Termin dostawy 20%	<p>Kryterium „Termin dostawy” – maksymalnie 20 punktów</p> <p>Zamawiający wymaga, aby przedmiot zamówienia został zrealizowany w terminie maksymalnie do 14 dni kalendarzowych licząc od daty zawarcia umowy (dotyczy wszystkich części)</p> <p>W powyższym kryterium oceniana będzie łączna długość terminu dostawy od dnia podpisania umowy. Zamawiający odniesie wartości z poszczególnych ofert do minimalnego oczekiwanego przez Zamawiającego terminu dostawy, min 7 dni, natomiast nie może być on dłuższy niż 14 dni.</p> $TD = (14 \text{ dni} - Tob) : 7 \text{ dni} \times 20 \text{ pkt}$ <p>gdzie: TD – przyznane punkty; Tob – termin oferty badanej (wyrażony w dniach).</p> <p>2) Każdy wykonawca będzie oceniany w kryterium „termin dostawy” w skali od 0 do 20 punktów</p> <p>UWAGA!!!</p> <ul style="list-style-type: none"> Zamawiający informuje, że w przypadku określenia przez Wykonawcę terminu dostawy krótszego niż 7 dni, Zamawiający przyjmie do obliczeń w kryterium oceny ofert „Termin



	<p>dostawy” wartość 7 dni, natomiast termin wskazany przez Wykonawcę będzie wiążący do realizacji przez Niego zamówienia.</p> <ul style="list-style-type: none"> • W przypadku określenia przez Wykonawcę terminu dostawy dłuższego niż 14 dni, oferta będzie odrzucona, jako niezgodna z SIWZ. • Termin dostawy będzie liczony od dnia zawarcia umowy. <p>Brak wskazania/wpisania w Formularzu oferty terminu dostawy, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca oferuje najdłuższy (maksymalny akceptowany przez Zamawiającego) termin dostawy, czyli 14 dni</p> <p>Zaoferowanie terminu realizacji niezgodnego z wytycznymi Zamawiającego będzie skutkować odrzuceniem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p> <p>Wykonawca zobowiązany jest w ofercie wyrazić oferowany termin realizacji w dniach. W przypadku podania terminu realizacji w innej postaci Zamawiający dokona stosownych przeliczeń opierając się na postanowieniach Kodeksu cywilnego dotyczących tygodnia, miesiąca.</p> <p>Wykonawca w oferowanym terminie realizacji zamówienia musi uwzględnić wszelkie ryzyka jakie mógł przewidzieć doświadczony Wykonawca, a w szczególności ryzyka związane z realizacją przedmiotu zamówienia.</p>
<p>c) Wsparcie techniczne 20%</p>	<p><u>Wsparcie techniczne – 20%:</u> Punkty w tym kryterium zostaną przyznane w następujący sposób:</p> <ul style="list-style-type: none"> • <u>zaoferowanie rozszerzenia wsparcia technicznego przez producenta z 12 miesięcy na 24 miesiące -20 pkt</u> • <u>niezaoferowanie rozszerzenia wsparcia technicznego przez producenta z 12 miesięcy na 24 miesiące - 0 pkt</u> <p>UWAGA!!!!</p> <p>Zamawiający informuje, że kryterium ma charakter zero/jedynkowy, tzn. jeżeli Wykonawca oświadczy w złożonej ofercie, że oferuje „rozszerzenie wsparcia technicznego przez producenta z 12 miesięcy na 24 miesiące”, wówczas Zamawiający przyzna 20 pkt.</p> <p>Brak wskazania/wpisania w Formularzu oferty powyższego kryterium, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca jego nie oferuje, więc nie otrzyma punktów w tym kryterium.</p> <p>Zaoferowanie kryterium wsparcia technicznego niezgodnego z wytycznymi Zamawiającego będzie skutkować odrzuceniem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p>

Łączna liczba punktów za kryterium cenowe, termin dostawy oraz wsparcie techniczne liczona będzie wzorem:

$$LP = LP_c + LP_{td} + LP_{wt}$$

gdzie:

- LP to liczba punktów
 LP_c to kryterium cenowe
 LP_{td} to kryterium terminu dostawy
 LP_{wt} to kryterium wsparcia technicznego

CZĘŚĆ 5

Waga kryterium	Opis kryterium oceny ofert
<p>b) Termin gwarancji 20%</p>	<p><u>Termin gwarancji – 20%:</u> Punkty w tym kryterium zostaną przyznane w następujący sposób:</p> <ul style="list-style-type: none"> • <u>zaoferowanie rozszerzenia gwarancji z 24 miesięcy na 36 miesięcy producenta -20 pkt</u>

	<ul style="list-style-type: none"> • <u>niezaoferowanie rozszerzenia gwarancji z 24 miesięcy na 36 miesięcy producenta - 0 pkt</u> <p>UWAGA!!!! Zamawiający informuje, że kryterium ma charakter zero/jedynkowy, tzn. jeżeli Wykonawca oświadczy w złożonej ofercie, że oferuje „rozszerzenie gwarancji z 24 miesięcy na 36 miesięcy producenta”, wówczas Zamawiający przyzna 20 pkt. Brak wskazania/wpisania w Formularzu oferty powyższego kryterium, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca jego nie oferuje, więc nie otrzyma punktów w tym kryterium. Zaoferowanie kryterium terminu gwarancji niezgodnego z wytycznymi Zamawiającego będzie skutkowało odrzuceniem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p>
<p>c) Kryterium jakościowe 20%</p>	<p><u>Kryterium jakościowe – 20%:</u> Wykonawca otrzyma największą ilość punktów za dostarczenie karty graficznej z kablem wysokiej jakości wykonania DVI-HDMI 1,8 m. Punkty będą liczone w następujący sposób:</p> <ul style="list-style-type: none"> • <u>zaoferowanie karty graficznej z kablem wysokiej jakości wykonania DVI-HDMI 1,8 m przez Wykonawcę -20 pkt</u> • <u>niezaoferowanie karty graficznej z kablem wysokiej jakości wykonania DVI-HDMI 1,8 m przez Wykonawcę - 0 pkt</u> <p>UWAGA!!!! Zamawiający informuje, że kryterium ma charakter zero/jedynkowy, tzn. jeżeli Wykonawca oświadczy w złożonej ofercie, że oferuje „kartę graficzną z kablem”, wówczas Zamawiający przyzna 20 pkt. Brak wskazania/wpisania w Formularzu oferty powyższego kryterium, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca jego nie oferuje, więc nie otrzyma punktów w tym kryterium. Zaoferowanie kryterium jakościowego niezgodnego z wytycznymi Zamawiającego będzie skutkowało odrzuceniem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p>

Łączna liczba punktów za kryterium cenowe, termin gwarancji oraz kryterium jakościowe liczona będzie wzorem:

$$LP = LP_c + LP_g + LP_{kj}$$

gdzie:

- LP to liczba punktów
 LP_c to kryterium cenowe
 LP_g to termin gwarancji
 LP_{kj} to kryterium jakościowe

CZĘŚĆ 6

Waga kryterium	Opis kryterium oceny ofert
<p>d) Termin gwarancji 20%</p>	<p><u>Termin gwarancji – 20%:</u> Punkty w tym kryterium zostaną przyznane w następujący sposób:</p> <ul style="list-style-type: none"> • <u>zaoferowanie rozszerzenia gwarancji z 24 miesięcy na 60 miesięcy producenta -20 pkt</u> • <u>niezaoferowanie rozszerzenia gwarancji z 24 miesięcy na 60 miesięcy producenta - 0 pkt</u> <p>UWAGA!!!! Zamawiający informuje, że kryterium ma charakter zero/jedynkowy, tzn. jeżeli Wykonawca oświadczy w złożonej ofercie, że oferuje „rozszerzenie gwarancji z 24 miesięcy na 60 miesięcy producenta”, wówczas Zamawiający przyzna 20 pkt.</p>

	Brak wskazania/wpisania w Formularzu oferty powyższego kryterium, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca jego nie oferuje, więc nie otrzyma punktów w tym kryterium. Zaoferowanie kryterium terminu gwarancji niezgodnego z wytycznymi Zamawiającego będzie skutkowało odrzuceniem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.
e) Kryterium jakościowe 20%	<p><u>Kryterium jakościowe – 20%:</u> Wykonawca otrzyma największą ilość punktów za dostarczenie do każdego dysku ramek umożliwiających zamontowanie dysku twardego SSD o wielkości 2,5 cala do zatoki 3,5 cala w komputerach PC. Punkty będą liczone w następujący sposób:</p> <ul style="list-style-type: none"> • <u>zaoferowanie do każdego dysku ramek przez Wykonawcę -20 pkt</u> • <u>niezaoferowanie do każdego dysku ramek przez Wykonawcę - 0 pkt</u> <p>UWAGA!!!! Zamawiający informuje, że kryterium ma charakter zero/jedynkowy, tzn. jeżeli Wykonawca oświadczy w złożonej ofercie, że oferuje „do każdego dysku ramki”, wówczas Zamawiający przyzna 20 pkt. Brak wskazania/wpisania w Formularzu oferty powyższego kryterium, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca jego nie oferuje, więc nie otrzyma punktów w tym kryterium. Zaoferowanie kryterium jakościowego niezgodnego z wytycznymi Zamawiającego będzie skutkowało odrzuceniem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p>

Łączna liczba punktów za kryterium cenowe, termin gwarancji oraz kryterium jakościowe liczona będzie wzorem:

$$LP = LP_c + LP_g + LP_{kj}$$

gdzie:

LP to liczba punktów
 LP_c to kryterium cenowe
 LP_g to termin gwarancji
 LP_{kj} to kryterium jakościowe

CZĘŚĆ 7

Waga kryterium	Opis kryterium oceny ofert
b) Termin gwarancji 20%	<p><u>Termin gwarancji – 20%:</u> Punkty w tym kryterium zostaną przyznane w następujący sposób:</p> <ul style="list-style-type: none"> • <u>zaoferowanie rozszerzenia gwarancji z 24 miesięcy na 60 miesięcy producenta -20 pkt</u> • <u>niezaoferowanie rozszerzenia gwarancji z 24 miesięcy na 60 miesięcy producenta - 0 pkt</u> <p>UWAGA!!!! Zamawiający informuje, że kryterium ma charakter zero/jedynkowy, tzn. jeżeli Wykonawca oświadczy w złożonej ofercie, że oferuje „rozszerzenie gwarancji z 24 miesięcy na 60 miesięcy”, wówczas Zamawiający przyzna 20 pkt. Brak wskazania/wpisania w Formularzu oferty powyższego kryterium, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca jego nie oferuje, więc nie otrzyma punktów w tym kryterium. Zaoferowanie kryterium terminu gwarancji niezgodnego z wytycznymi Zamawiającego będzie skutkowało odrzuceniem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p>
c) Termin dostawy 20%	<p>Kryterium „Termin dostawy” – maksymalnie 20 punktów Zamawiający wymaga, aby przedmiot zamówienia został zrealizowany w terminie maksymalnie do 14 dni kalendarzowych licząc od daty zawarcia umowy (dotyczy</p>

	<p>wszystkich części)</p> <p>W powyższym kryterium oceniana będzie łączna długość terminu dostawy od dnia podpisania umowy. Zamawiający odniesie wartości z poszczególnych ofert do minimalnego oczekiwanego przez Zamawiającego terminu dostawy, min 7 dni, natomiast nie może być on dłuższy niż 14 dni.</p> $TD = (14 \text{ dni} - Tob) : 7 \text{ dni} \times 20 \text{ pkt}$ <p>gdzie:</p> <p>TD – przyznane punkty;</p> <p>Tob – termin oferty badanej (wyrażony w dniach).</p> <p>2) Każdy wykonawca będzie oceniany w kryterium „termin dostawy” w skali od 0 do 20 punktów</p> <p>UWAGA!!!</p> <ul style="list-style-type: none"> • Zamawiający informuje, że w przypadku określenia przez Wykonawcę terminu dostawy krótszego niż 7 dni, Zamawiający przyjmie do obliczeń w kryterium oceny ofert „Termin dostawy” wartość 7 dni, natomiast termin wskazany przez Wykonawcę będzie wiążący do realizacji przez Niego zamówienia. • W przypadku określenia przez Wykonawcę terminu dostawy dłuższego niż 14 dni, oferta będzie odrzucona, jako niezgodna z SIWZ. • Termin dostawy będzie liczony od dnia zawarcia umowy. <p>Brak wskazania/wpisania w Formularzu oferty terminu dostawy, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca oferuje najdłuższy (maksymalny akceptowany przez Zamawiającego) termin dostawy, czyli 14 dni</p> <p>Zaoferowanie terminu realizacji niezgodnego z wytycznymi Zamawiającego będzie skutkować odrzuceniem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p> <p>Wykonawca zobowiązany jest w ofercie wyrazić oferowany termin realizacji w dniach. W przypadku podania terminu realizacji w innej postaci Zamawiający dokona stosownych przeliczeń opierając się na postanowieniach Kodeksu cywilnego dotyczących tygodnia, miesiąca.</p> <p>Wykonawca w oferowanym terminie realizacji zamówienia musi uwzględnić wszelkie ryzyka jakie mógł przewidzieć doświadczony Wykonawca, a w szczególności ryzyka związane z realizacją przedmiotu zamówienia.</p>
--	--

Łączna liczba punktów za kryterium cenowe, termin gwarancji oraz kryterium termin dostawy będzie wzorem:

$$LP = LP_c + LP_g + LP_{td}$$

gdzie:

LP to liczba punktów

LP_c to kryterium cenowe

LP_g to termin gwarancji

LP_{td} to kryterium termin dostawy

CZĘŚĆ 8

Waga kryterium	Opis kryterium oceny ofert
b) Termin gwarancji 20%	<p><u>Termin gwarancji – 20%:</u> Punkty w tym kryterium zostaną przyznane w następujący sposób:</p> <ul style="list-style-type: none"> • <u>zaoferowanie rozszerzenia gwarancji z 36 miesięcy na 60 miesięcy producenta -20 pkt</u> • <u>niezaoferowanie rozszerzenia gwarancji z 36 miesięcy na 60 miesięcy producenta - 0 pkt</u> <p>UWAGA!!!! Zamawiający informuje, że kryterium ma charakter zero/jedynkowy, tzn. jeżeli Wykonawca oświadczy w złożonej ofercie, że oferuje „rozszerzenie gwarancji z 36 miesięcy na 60 miesięcy producenta”, wówczas Zamawiający przyzna 20 pkt. Brak wskazania/wpisania w Formularzu oferty powyższego kryterium, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca jego nie oferuje, więc nie otrzyma punktów w tym kryterium. Zaoferowanie kryterium terminu gwarancji niezgodnego z wytycznymi Zamawiającego będzie skutkowało odrzuceniem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p>
c) Kryterium jakościowe 20%	<p><u>Kryterium jakościowe – 20%:</u> Wykonawca otrzyma największą ilość punktów za dostarczenie adaptera z micro SD na kartę SD. Punkty będą liczone w następujący sposób:</p> <ul style="list-style-type: none"> • <u>zaoferowanie adaptera z micro SD na kartę SD przez Wykonawcę - 20 pkt</u> • <u>niezaoferowanie adaptera z micro SD na kartę SD przez Wykonawcę - 0 pkt</u> <p>UWAGA!!!! Zamawiający informuje, że kryterium ma charakter zero/jedynkowy, tzn. jeżeli Wykonawca oświadczy w złożonej ofercie, że oferuje „adaptera”, wówczas Zamawiający przyzna 20 pkt. Brak wskazania/wpisania w Formularzu oferty powyższego kryterium, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca jego nie oferuje, więc nie otrzyma punktów w tym kryterium. Zaoferowanie kryterium jakościowego niezgodnego z wytycznymi Zamawiającego będzie skutkowało odrzuceniem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p>

Łączna liczba punktów za kryterium cenowe, termin gwarancji oraz kryterium jakościowe liczona będzie wzorem:

$$LP = LP_c + LP_g + LP_{kj}$$

gdzie:

- LP to liczba punktów
 LP_c to kryterium cenowe
 LP_g to termin gwarancji
 LP_{kj} to kryterium jakościowe

CZEŚĆ 9

Waga kryterium	Opis kryterium oceny ofert
----------------	----------------------------



<p>b) Termin dostawy 20%</p>	<p>Kryterium „Termin dostawy” – maksymalnie 20 punktów Zamawiający wymaga, aby przedmiot zamówienia został zrealizowany w terminie maksymalnie do 14 dni kalendarzowych licząc od daty zawarcia umowy (dotyczy wszystkich części) W powyższym kryterium oceniana będzie łączna długość terminu dostawy od dnia podpisania umowy. Zamawiający odniesie wartości z poszczególnych ofert do minimalnego oczekiwanego przez Zamawiającego terminu dostawy, min 7 dni, natomiast nie może być on dłuższy niż 14 dni.</p> <p style="text-align: center;">$TD = (14 \text{ dni} - Tob) : 7 \text{ dni} \times 20 \text{ pkt}$</p> <p>gdzie: TD – przyznane punkty; Tob – termin oferty badanej (wyrażony w dniach).</p> <p>2) Każdy wykonawca będzie oceniany w kryterium „termin dostawy” w skali od 0 do 20 punktów</p> <p>UWAGA!!!</p> <ul style="list-style-type: none">• Zamawiający informuje, że w przypadku określenia przez Wykonawcę terminu dostawy krótszego niż 7 dni, Zamawiający przyjmie do obliczeń w kryterium oceny ofert „Termin dostawy” wartość 7 dni, natomiast termin wskazany przez Wykonawcę będzie wiążący do realizacji przez Niego zamówienia.• W przypadku określenia przez Wykonawcę terminu dostawy dłuższego niż 14 dni, oferta będzie odrzucona, jako niezgodna z SIWZ.• Termin dostawy będzie liczony od dnia zawarcia umowy. <p>Brak wskazania/wpisania w Formularzu oferty terminu dostawy, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca oferuje najdłuższy (maksymalny akceptowany przez Zamawiającego) termin dostawy, czyli 14 dni</p> <p>Zaferowanie terminu realizacji niezgodnego z wytycznymi Zamawiającego będzie skutkować odrzuceniem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ. Wykonawca zobowiązany jest w ofercie wyrazić oferowany termin realizacji w dniach. W przypadku podania terminu realizacji w innej postaci Zamawiający dokona stosownych przeliczeń opierając się na postanowieniach Kodeksu cywilnego dotyczących tygodnia, miesiąca. Wykonawca w oferowanym terminie realizacji zamówienia musi uwzględnić wszelkie ryzyka jakie mógł przewidzieć doświadczony Wykonawca, a w szczególności ryzyka związane z realizacją przedmiotu zamówienia.</p>
<p>c) Termin gwarancji 20%</p>	<p>Termin gwarancji – 20%: Punkty w tym kryterium zostaną przyznane w następujący sposób:</p> <ul style="list-style-type: none">• <u>zaferowanie rozszerzenia gwarancji z 36 miesięcy na 60 miesięcy producenta -20 pkt</u>• <u>niezaferowanie rozszerzenia gwarancji z 36 miesięcy na 60 miesięcy producenta - 0 pkt</u> <p>UWAGA!!!! Zamawiający informuje, że kryterium ma charakter zero/jedynkowy, tzn. jeżeli Wykonawca oświadczy w złożonej ofercie, że oferuje „rozszerzenie gwarancji z 36 miesięcy na 60 miesięcy producenta”, wówczas Zamawiający przyzna 20 pkt. Brak wskazania/wpisania w Formularzu oferty powyższego kryterium, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca jego nie oferuje, więc nie otrzyma punktów w tym kryterium. Zaferowanie kryterium terminu gwarancji niezgodnego z wytycznymi Zamawiającego będzie skutkować odrzuceniem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p>

--	--

Łączna liczba punktów za kryterium cenowe, termin dostawy oraz termin gwarancji liczona będzie wzorem:

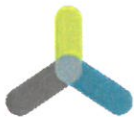
$$LP = LP_c + LP_{td} + LP_g$$

gdzie:

- LP to liczba punktów
 LP_c to kryterium cenowe
 LP_{td} to kryterium terminu dostawy
 LP_g to termin gwarancji

CZĘŚĆ 10

Waga kryterium	Opis kryterium oceny ofert
b) Termin dostawy 20%	<p>Kryterium „Termin dostawy” – maksymalnie 20 punktów Zamawiający wymaga, aby przedmiot zamówienia został zrealizowany w terminie maksymalnie do 14 dni kalendarzowych licząc od daty zawarcia umowy (dotyczy wszystkich części) W powyższym kryterium oceniana będzie łączna długość terminu dostawy od dnia podpisania umowy. Zamawiający odniesie wartości z poszczególnych ofert do minimalnego oczekiwanego przez Zamawiającego terminu dostawy, min 5 dni, natomiast nie może być on dłuższy niż 14 dni.</p> <p style="text-align: center;">$TD = (14 \text{ dni} - Tob) : 9 \text{ dni} \times 20 \text{ pkt}$</p> <p>gdzie: TD – przyznane punkty; Tob – termin oferty badanej (wyrażony w dniach).</p> <p>2) Każdy wykonawca będzie oceniany w kryterium „termin dostawy” w skali od 0 do 20 punktów</p> <p>UWAGA!!!</p> <ul style="list-style-type: none"> • Zamawiający informuje, że w przypadku określenia przez Wykonawcę terminu dostawy krótszego niż 5 dni, Zamawiający przyjmie do obliczeń w kryterium oceny ofert „Termin dostawy” wartość 5 dni, natomiast termin wskazany przez Wykonawcę będzie wiążący do realizacji przez Niego zamówienia. • W przypadku określenia przez Wykonawcę terminu dostawy dłuższego niż 14 dni, oferta będzie odrzucona, jako niezgodna z SIWZ. • Termin dostawy będzie liczony od dnia zawarcia umowy. <p>Brak wskazania/wpisania w Formularzu oferty terminu dostawy, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca oferuje najdłuższy (maksymalny akceptowany przez Zamawiającego) termin dostawy, czyli 14 dni</p> <p>Zaoferowanie terminu realizacji niezgodnego z wytycznymi Zamawiającego będzie skutkować</p>



	<p>odrzuconiem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ. Wykonawca zobowiązany jest w ofercie wyrazić oferowany termin realizacji w dniach. W przypadku podania terminu realizacji w innej postaci Zamawiający dokona stosownych przeliczeń opierając się na postanowieniach Kodeksu cywilnego dotyczących tygodnia, miesiąca. Wykonawca w oferowanym terminie realizacji zamówienia musi uwzględnić wszelkie ryzyka jakie mógł przewidzieć doświadczony Wykonawca, a w szczególności ryzyka związane z realizacją przedmiotu zamówienia.</p>
c) Kryterium jakościowe 20%	<p><u>Kryterium jakościowe – 20%:</u> Punkty w tym kryterium zostaną przyznane w następujący sposób:</p> <ul style="list-style-type: none"> • <u>zaoferowanie dodatkowych dwóch licencji na oprogramowanie do ochrony urządzeń mobilnych -20 pkt</u> • <u>niezaoferowanie dodatkowych dwóch licencji na oprogramowanie do ochrony urządzeń mobilnych - 0 pkt</u> <p>UWAGA!!!! Zamawiający informuje, że kryterium ma charakter zero/jedynkowy, tzn. jeżeli Wykonawca oświadczy w złożonej ofercie, że oferuje „dodatkowo dwie licencje” wówczas Zamawiający przyzna 20 pkt. Brak wskazania/wpisania w Formularzu oferty powyższego kryterium, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca jego nie oferuje, więc nie otrzyma punktów w tym kryterium. Zaoferowanie kryterium jakościowego niezgodnego z wytycznymi Zamawiającego będzie skutkowało odrzuconiem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p>

Łączna liczba punktów za kryterium cenowe, termin dostawy oraz kryterium jakościowe liczona będzie wzorem:

$$LP = LP_c + LP_{td} + LP_{kj}$$

gdzie:

- LP to liczba punktów
 LP_c to kryterium cenowe
 LP_{td} to kryterium terminu dostawy
 LP_{kj} to kryterium jakościowe

CZĘŚĆ 11

Waga kryterium	Opis kryterium oceny ofert
b) Termin gwarancji 20%	<p><u>Termin gwarancji – 20%:</u> Punkty w tym kryterium zostaną przyznane w następujący sposób:</p> <ul style="list-style-type: none"> • <u>zaoferowanie rozszerzenia gwarancji z 24 miesięcy na 36 miesięcy producenta - następnego dnia roboczego, naprawa u klienta -20 pkt</u> • <u>niezaoferowanie rozszerzenia gwarancji z 24 miesięcy na 36 miesięcy producenta- następnego dnia roboczego, naprawa u klienta - 0 pkt</u> <p>UWAGA!!!! Zamawiający informuje, że kryterium ma charakter zero/jedynkowy, tzn. jeżeli Wykonawca oświadczy w złożonej ofercie, że oferuje „rozszerzenie gwarancji z 24 miesięcy na 36 miesięcy producenta – następnego dnia roboczego, naprawa u klienta”, wówczas Zamawiający przyzna 20 pkt. Brak wskazania/wpisania w Formularzu oferty powyższego kryterium, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca jego nie oferuje, więc nie otrzyma punktów w tym kryterium. Zaoferowanie kryterium terminu gwarancji niezgodnego z wytycznymi Zamawiającego będzie skutkowało odrzuconiem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p>

	odrzuconiem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.
c) Kryterium jakościowe 20%	<p><u>Kryterium jakościowe – 20%:</u> Wykonawca otrzyma największą ilość punktów za dostarczenie dodatkowo klawiatury i myszy bezprzewodowej. Klawiatura: klawisze - cicha praca, małym skokiem, multimedialne, funkcyjne, podpórka pod nadgarstki, wyłącznik na przednim panelu klawiatury. Mysz: sensor – optyczny, 3 przyciski, rolka przewijania, rozdzielczość-1000dpi. Zaawansowane śledzenie optyczne. Punkty będą liczone w następujący sposób:</p> <ul style="list-style-type: none"> • <u>zaoferowanie dodatkowo klawiatury i myszy bezprzewodowej przez Wykonawcę -20 pkt</u> • <u>niezaoferowanie dodatkowo klawiatury i myszy bezprzewodowej przez Wykonawcę - 0 pkt</u> <p>UWAGA!!!! Zamawiający informuje, że kryterium ma charakter zero/jedynkowy, tzn. jeżeli Wykonawca oświadczy w złożonej ofercie, że oferuje „dodatkowo klawiaturę i mysz bezprzewodowej”, wówczas Zamawiający przyzna 20 pkt. Brak wskazania/wpisania w Formularzu oferty powyższego kryterium, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca jego nie oferuje, więc nie otrzyma punktów w tym kryterium. Zaoferowanie kryterium jakościowego niezgodnego z wytycznymi Zamawiającego będzie skutkowało odrzuconiem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p>

Łączna liczba punktów za kryterium cenowe, termin gwarancji oraz kryterium jakościowe liczona będzie wzorem:

$$LP = LP_c + LP_g + LP_{kj}$$

gdzie:

LP to liczba punktów
 LP_c to kryterium cenowe
 LP_g to termin gwarancji
 LP_{kj} to kryterium jakościowe

CZĘŚĆ 12

Waga kryterium	Opis kryterium oceny ofert
b) Termin gwarancji 20%	<p><u>Termin gwarancji – 20%:</u> Punkty w tym kryterium zostaną przyznane w następujący sposób:</p> <ul style="list-style-type: none"> • <u>zaoferowanie rozszerzenia gwarancji monitora z 36 miesięcy na 60 miesięcy producenta -20 pkt</u> • <u>niezaoferowanie rozszerzenia gwarancji monitora z 36 miesięcy na 60 miesięcy producenta - 0 pkt</u> <p>UWAGA!!!! Zamawiający informuje, że kryterium ma charakter zero/jedynkowy, tzn. jeżeli Wykonawca oświadczy w złożonej ofercie, że oferuje „rozszerzenie gwarancji z 36 miesięcy na 60 miesięcy”, wówczas Zamawiający przyzna 20 pkt. Brak wskazania/wpisania w Formularzu oferty powyższego kryterium, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca jego nie oferuje, więc nie otrzyma punktów w tym kryterium. Zaoferowanie kryterium terminu gwarancji niezgodnego z wytycznymi Zamawiającego będzie skutkowało odrzuconiem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p>

	odrzuconiem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.
c) Kryterium jakościowe 20%	<p><u>Kryterium jakościowe – 20%:</u> Wykonawca otrzyma największą ilość punktów za dostarczenie kabla wysokiej jakości DVI męska-HDMI 1,8 m, pozłacane końcówki złącz. Punkty będą liczone w następujący sposób:</p> <ul style="list-style-type: none"> • <u>zaoferowanie kabla DVI męska- HDMI przez Wykonawcę -20 pkt</u> • <u>niezaoferowanie kabla DVI męska- HDMI przez Wykonawcę - 0 pkt</u> <p>UWAGA!!!! Zamawiający informuje, że kryterium ma charakter zero/jedynkowy, tzn. jeżeli Wykonawca oświadczy w złożonej ofercie, że oferuje „kable”, wówczas Zamawiający przyzna 20 pkt. Brak wskazania/wpisania w Formularzu oferty powyższego kryterium, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca jego nie oferuje, więc nie otrzyma punktów w tym kryterium. Zaoferowanie kryterium jakościowego niezgodnego z wytycznymi Zamawiającego będzie skutkowało odrzuconiem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p>

Łączna liczba punktów za kryterium cenowe, termin gwarancji oraz kryterium jakościowe liczona będzie wzorem:

$$LP = LP_c + LP_g + LP_{kj}$$

gdzie:

- LP to liczba punktów
 LP_c to kryterium cenowe
 LP_g to termin gwarancji
 LP_{kj} to kryterium jakościowe

CZEŚĆ 14

Waga kryterium	Opis kryterium oceny ofert
c) Termin gwarancji 20%	<p><u>Termin gwarancji – 20%:</u> Punkty w tym kryterium zostaną przyznane w następujący sposób:</p> <ul style="list-style-type: none"> • <u>zaoferowanie rozszerzenia gwarancji z 24 miesięcy na 36 miesięcy producenta -20 pkt</u> • <u>niezaoferowanie rozszerzenia gwarancji z 24 miesięcy na 36 miesięcy producenta - 0 pkt</u> <p>UWAGA!!!! Zamawiający informuje, że kryterium ma charakter zero/jedynkowy, tzn. jeżeli Wykonawca oświadczy w złożonej ofercie, że oferuje „rozszerzenie gwarancji z 24 miesięcy na 36 miesięcy”, wówczas Zamawiający przyzna 20 pkt. Brak wskazania/wpisania w Formularzu oferty powyższego kryterium, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca jego nie oferuje, więc nie otrzyma punktów w tym kryterium. Zaoferowanie kryterium terminu gwarancji niezgodnego z wytycznymi Zamawiającego będzie skutkowało odrzuconiem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p>
c) Termin dostawy 20%	<p>Kryterium „Termin dostawy” – maksymalnie 20 punktów Zamawiający wymaga, aby przedmiot zamówienia został zrealizowany w terminie maksymalnie do 14 dni kalendarzowych licząc od daty zawarcia umowy (dotyczy</p>

	<p>wszystkich części)</p> <p>W powyższym kryterium oceniana będzie łączna długość terminu dostawy od dnia podpisania umowy. Zamawiający odniesie wartości z poszczególnych ofert do minimalnego oczekiwanego przez Zamawiającego terminu dostawy, min 7 dni, natomiast nie może być on dłuższy niż 14 dni.</p> $TD = (14 \text{ dni} - Tob) : 7 \text{ dni} \times 20 \text{ pkt}$ <p>gdzie:</p> <p>TD – przyznane punkty; Tob – termin oferty badanej (wyrażony w dniach).</p> <p>2) Każdy wykonawca będzie oceniany w kryterium „termin dostawy” w skali od 0 do 20 punktów</p> <p>UWAGA!!!</p> <ul style="list-style-type: none"> • Zamawiający informuje, że w przypadku określenia przez Wykonawcę terminu dostawy krótszego niż 7 dni, Zamawiający przyjmie do obliczeń w kryterium oceny ofert „Termin dostawy” wartość 7 dni, natomiast termin wskazany przez Wykonawcę będzie wiążący do realizacji przez Niego zamówienia. • W przypadku określenia przez Wykonawcę terminu dostawy dłuższego niż 14 dni, oferta będzie odrzucona, jako niezgodna z SIWZ. • Termin dostawy będzie liczony od dnia zawarcia umowy. <p>Brak wskazania/wpisania w Formularzu oferty terminu dostawy, skutkować będzie przyjęciem przez Zamawiającego, że Wykonawca oferuje najdłuższy (maksymalny akceptowany przez Zamawiającego) termin dostawy, czyli 14 dni</p> <p>Zaoferowanie terminu realizacji niezgodnego z wytycznymi Zamawiającego będzie skutkowało odrzuceniem oferty zgodnie z art. 89 ust. 1 pkt 2 ustawy Pzp, jako niezgodnej z treścią SIWZ.</p> <p>Wykonawca zobowiązany jest w ofercie wyrazić oferowany termin realizacji w dniach. W przypadku podania terminu realizacji w innej postaci Zamawiający dokona stosownych przeliczeń opierając się na postanowieniach Kodeksu cywilnego dotyczących tygodnia, miesiąca.</p> <p>Wykonawca w oferowanym terminie realizacji zamówienia musi uwzględnić wszelkie ryzyka jakie mógł przewidzieć doświadczony Wykonawca, a w szczególności ryzyka związane z realizacją przedmiotu zamówienia.</p>
--	--

Łączna liczba punktów za kryterium cenowe, termin gwarancji oraz kryterium termin dostawy będzie wzorem:

$$LP = LP_c + LP_g + LP_{td}$$

gdzie:

LP to liczba punktów
 LP_c to kryterium cenowe
 LP_g to termin gwarancji
 LP_{td} to kryterium termin dostawy

Dotyczy każdej z części:

1. Punkty za kryteria: cena oferty i kryteria jakościowe zostaną zsumowane.
2. Każdy wykonawca będzie oceniany w skali od 0 do 100 punktów.
3. Liczba punktów zostanie zaokrąglona do 2 miejsc po przecinku.
4. Punktacja przyznawana ofertom w poszczególnych kryteriach będzie liczona z dokładnością do dwóch miejsc po przecinku (zasada zaokrąglenia – trzecie miejsce po przecinku, poniżej 5 końcówka zostanie pominięta, powyżej i równe 5 końcówka zostanie zaokrąglona w górę). Najwyższa liczba punktów wyznaczy najkorzystniejszą ofertę.
5. Zamawiający udzieli zamówienia wykonawcy, którego oferta odpowiadać będzie wszystkim wymaganiom przedstawionym w ustawie Pzp, oraz SIWZ i zostanie oceniona jako najkorzystniejsza w oparciu o podane kryteria wyboru.
6. Zamawiający zgodnie z art. 24 aa ustawy pzp może najpierw dokonać oceny ofert, a następnie zbadać, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.
7. Jeżeli Wykonawca, o którym mowa w ust. 6, uchyla się od zawarcia umowy, Zamawiający może zbadać, czy nie podlega wykluczeniu oraz czy spełnia warunki udziału w postępowaniu Wykonawca, który złożył ofertę najwyższą ocenioną spośród pozostałych ofert. Punkty zostaną przyznane na podstawie informacji uzyskanych z formularza ofertowego stanowiącego Załącznik nr 2 do SIWZ.
8. Jeżeli nie będzie można dokonać wyboru najkorzystniejszej oferty ze względu na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i pozostałych kryteriów oceny ofert, Zamawiający spośród tych ofert dokona wyboru oferty z niższą ceną, zgodnie z art. 91 ust. 4 ustawy Pzp.
9. Zamawiający nie przewiduje przeprowadzenia dogrywki w formie aukcji elektronicznej.

XIV. INFORMACJA O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO.

1) Informacje o formalnościach, jakie powinny być spełnione w celu zawarcia umowy:

1. O wyborze najkorzystniejszej oferty Zamawiający informuje w trybie art. 92 ust. 1 niezwłocznie wszystkich Wykonawców, którzy złożyli ofertę.
2. Informacje o wyborze najkorzystniejszej oferty Zamawiający zamieszcza również na swojej stronie internetowej, zgodnie z art. 92 ust. 2 ustawy
3. Jeżeli jako najkorzystniejsza zostanie wybrana oferta Wykonawców – Konsorcjum/Spółki cywilnej, Zamawiający może żądać przed zawarciem umowy w sprawie zamówienia publicznego, umowy regulującej współpracę tych Wykonawców. Umowa regulująca współpracę tych podmiotów powinna zawierać: określenie celu gospodarczego, oświadczenia podmiotów o przyjęciu odpowiedzialności solidarnej, wskazanie podmiotu, któremu powierza się prowadzenie spraw i reprezentację na zewnątrz (lidera), oznaczenie czasu trwania umowy – wymaga się, aby czas trwania umowy był nie krótszy niż okres realizacji zamówienia. Umowa regulująca współpracę musi być podpisana tak, by zobowiązywała prawnie wszystkie podmioty gospodarcze oraz musi stwierdzać solidarną odpowiedzialność partnerów wobec Zamawiającego za wykonanie umowy.
4. Wykonawca, przed podpisaniem umowy, zobowiązuje się do przedłożenia Zamawiającemu informacji o podwykonawcach i zakresie prac, które zamierza im



- powierzyć w toku wykonywania zamówienia wraz z orientacyjną wartością powierzonych podwykonawcom prac – jeżeli dotyczy.
5. Jeżeli Wykonawca, którego oferta została wybrana, uchyla się od zawarcia umowy w sprawie zamówienia publicznego, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzenia ich ponownego badania i oceny, chyba, że zachodzą przesłanki unieważnienia postępowania, o których mowa w art. 93 ust. 1 ustawy.
 6. Przed podpisaniem umowy Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza na wezwanie Zamawiającego przedstawi szczegółową kalkulację ceny uwzględniającą kwotę netto oraz brutto na każdy asortyment przedmiotu zamówienia (wartość brutto musi być identyczna z wartością podaną na formularzu ofertowym) zgodnie z § 5 Wzoru umowy, stanowiącym załącznik nr 5.1; 5.2; 5.3 do SIWZ.
 7. Zamawiający będzie zawierał stosowne umowy o realizację zamówienia publicznego osobno dla każdej części, z wybranym wykonawcą.
 8. Wykonawca ma obowiązek zawrzeć umowę zgodnie ze wzorami umów stanowiącym załącznik nr 5.1; 5.2; 5.3 do SIWZ.
 9. Zawarta umowa będzie jawna i będzie podlegała udostępnianiu na zasadach określonych w przepisach o dostępie do informacji publicznej (art. 139 ust. 3 ustawy).

2) Termin i miejsce zawarcia umowy.

1. Zamawiający zawrze umowę w sprawie zamówienia publicznego, z zastrzeżeniem art. 183 ustawy, 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 - w przypadku zamówień, których wartość jest mniejsza niż kwoty określone w przepisach wydanych na podstawie art. 11 ust. 8.
2. Umowa zostanie zawarta w siedzibie Zamawiającego, przed upływem terminu związania ofertą.
3. Osoby reprezentujące Wykonawcę przy podpisywaniu umowy powinny posiadać ze sobą dokumenty potwierdzające ich umocowanie do podpisania umowy, o ile umocowanie to nie będzie wynikać z dokumentów załączonych do oferty.

XV. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY.

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

XVI. ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI ZAWIERANEJ UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO:



- 1) Wzory umów stanowią odpowiednio: załącznik nr 5.1; 5.2; 5.3 do SIWZ które stanowią integralną część SIWZ, w której Zamawiający przewidział wszystkie istotne dla stron postanowienia oraz przyszłe zobowiązania Wykonawcy i Zamawiającego.
- 2) Umowa/y zostanie/ą zawarta/e z uwzględnieniem postanowień wynikających z treści SIWZ oraz danych zawartych w ofercie.

XVII. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA :

1. Każdemu 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, przysługują odpowiednio środki ochrony prawnej, o których mowa w dziale VI ustawy jak dla postępowań poniżej kwoty określonej w przepisach wykonawczych wydanych na podstawie art. 11 ust. 3 ustawy Pzp.
2. Zgodnie z art. 179 ust. 1 ustawy Pzp „Środki ochrony prawnej określone w niniejszym dziale przysługują wykonawcy, uczestnikowi konkursu, 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 niniejszej ustawy”.
3. Zgodnie z art. 179 ust. 2 ustawy Pzp „Środki ochrony prawnej wobec ogłoszenia o zamówieniu oraz specyfikacji istotnych warunków zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 154 pkt 5 ustawy Pzp.
4. Odwołanie na podstawie art. 180 ust. 2 przysługuje wyłącznie wobec czynności:
 - 1) wyboru trybu negocjacji bez ogłoszenia, zamówienia z wolnej ręki lub zapytania o cenę;
 - 2) określenia warunków udziału w postępowaniu;
 - 3) wykluczenia odwołującego z postępowania o udzielenie zamówienia;
 - 4) odrzucenia oferty odwołującego;
 - 5) opisu przedmiotu zamówienia;
 - 6) wyboru najkorzystniejszej oferty;
5. Zgodnie z art. 182 ust. 1 pkt 2) ustawy odwołanie wnosi się 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 ustawy zdanie drugie, albo w terminie 10 dni – jeżeli zostały przesłane w inny sposób. Odwołanie wnosi się do Prezesa Izby (art. 180 ust. 4 ustawy).
6. Na podstawie art. 181 ust. 1 ustawy Wykonawca może poinformować Zamawiającego w terminie przewidzianym do wniesienia odwołania 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.

7. Skarga do sądu – zgodnie z art. 198a ust. 1 na orzeczenie Krajowej Izby Odwoławczej stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargę wnosi się do sądu okręgowego właściwego dla siedziby albo miejsca zamieszkania Zamawiającego (art. 198b ust. 1 ustawy). Skargę wnosi się za pośrednictwem Prezesa Izby w terminie 7 dni od dnia doręczenia orzeczenia Izby (art. 198b ust. 2 ustawy).
8. Zasady i tryb postępowania w zakresie korzystania ze środków ochrony prawnej określone zostały w dziale VI ustawy.
9. Środki ochrony prawnej wobec ogłoszenia o zamówieniu oraz SIWZ przysługują również organizacjom wpisanym na listę, o której mowa w art. 154 pkt 5 ustawy Pzp.

Załączniki do SIWZ:

Załącznik nr 1.1-1.14 – Szczegółowy opis przedmiotu zamówienia (część 1-14)

Załącznik nr 2 – Formularz oferty

Załącznik nr 3 A – Oświadczenie Wykonawcy A

Załącznik nr 3 B – Oświadczenie Wykonawcy B

Załącznik nr 4 – Wzór oświadczenia Wykonawcy o przynależności lub braku przynależności do grupy kapitałowej, o której mowa w art.24 ust. 11
(NALEŻY PRZEKAZAĆ ZAMAWIAJACEMU W CIĄGU 3 DNI OD DNIA PRZEKAZANIA INFORMACJI, O KTÓRYCH MOWA W ART. 86 UST. 5 USTAWY PZP)

Załącznik nr 5.1 - Wzór umowy (część 1 i 11)

Załącznik nr 5.2 - Wzór umowy (część 5; 6; 7; 8; 9; 12; 13; 14)

Załącznik nr 5.3 - Wzór umowy (część 2; 3; 4; 10)

Załącznik nr 6.1-6.14 – Zestawienie wymaganych parametrów technicznych i użytkowych (część 1-14)

D Y R E K T O R
Stawiński
prof. dr hab. Cezary Stawiński

Załącznik nr 1.1 – Szczegółowy opis przedmiotu zamówienia (część 1)

Część 1 – Dostawa komputerów PC laptopów – 9 szt.

1.1 Komputer PC laptop – 9 sztuk	
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:
Rodzaj laptopa	Wysoko wydajny ultrabook 14" Laptop wyposażony w oprogramowanie przeznaczone do: <ul style="list-style-type: none"> • Specjalistycznego oprogramowania, obliczeń, edytora tekstu poczty elektronicznej
Procesor	Procesor taktowany zegarem co najmniej 1,6 GHz, pamięci cache 6 MB lub równoważny procesor klasy x64 zapewniający spełnienie poniższych kryteriów wydajności: - wydajność całego oferowanego systemu komputerowego min. 1914pkt. w teście BAPCo MobileMark 2014 . Test MobileMark 2014 Results powinien być wykonany w konfiguracji całego laptopa identycznej z wymaganą oraz przy rozdzielczości ekranu co najmniej 1920 x 1080 pikseli i innymi ustawieniami zgodnymi z zaleceniami producenta testu.
Pamięć RAM	8 GB 2133 MHz LPDDR3
Dysk twarde	Dysk twarde zbudowany w oparciu o pamięć flash co najmniej 256 M.2 PCIe
Karta graficzna	Zintegrowana z procesorem ze wsparciem dla DirectX 12
Typ ekranu	14 cali, 1920 x 1080 (FullHD), matowy, bardzo szerokie kąty widzenia
Urządzenie wskazujące	Zintegrowana funkcja klawiszy numerycznych
Interfejsy komunikacyjne	Wi-Fi 802.11b/g/n/ac, Bluetooth,
Złącza	Wyjścia: HDMI – 1 szt., USB 3.0 - 1 szt., USB Typu-C - 1 szt., USB 2.0 – 1 szt., zintegrowana kamera internetowa, czytnik kart pamięci MicroSD
Wymiary	Waga max 1,2 kg, max. wysokość 16 mm
Bateria	9 h pracy
System operacyjny	Zainstalowany stabilny system operacyjny w języku polskim, zainstalowany na sprzęcie komputerowym objętym przedmiotem zamówienia przez producenta laptopa.
Dołączone akcesoria	Dedykowane przez tego samego producenta co urządzenie firmowe etui na laptopa Dedykowana przez producenta przejściówka USB -> RJ-45 Zasilacz
Dodatkowe informacje	<ul style="list-style-type: none"> • Białe podświetlenie klawiatury • Wielodotkowy, intuicyjny touchpad • Wbudowany czytnik linii papilarnych • Szyfrowanie TPM
Gwarancja na laptopa	12 miesięcy

Załącznik nr 1.2 – Szczegółowy opis przedmiotu zamówienia (część 2)

Część 2 – Dostawa licencji na uaktualnienie systemu operacyjnego do wersji profesjonalnej (wersja edukacyjna)– 8 szt.

2.1 Licencja na uaktualnienie systemu operacyjnego do wersji profesjonalnej (wersja edukacyjna) – 8 sztuk	
Upgrade	Licencja na podniesienie systemu operacyjnego do wersji profesjonalnej, edukacyjnej o następujących parametrach: w języku polskim, w pełni obsługujący pracę w domenie i kontrolę użytkowników w technologii ActiveDirectory, zcentralizowane zarządzanie oprogramowaniem i konfigurację systemu w technologii Group Policy.
Wsparcie techniczne	12 miesięcy

Załącznik nr 1.3 – Szczegółowy opis przedmiotu zamówienia (część 3)

Część 3 – Dostawa licencji na uaktualnienie systemu operacyjnego do wersji profesjonalnej EN (wersja edukacyjna)– 1 szt.

3.1 Licencja na uaktualnienie systemu operacyjnego do wersji profesjonalnej EN (wersja edukacyjna) – 1 sztuka	
Upgrade	Licencja na podniesienie systemu operacyjnego do wersji profesjonalnej, edukacyjnej o następujących parametrach: w języku angielskim, w pełni obsługujący pracę w domenie i kontrolę użytkowników w technologii ActiveDirectory, zcentralizowane zarządzanie oprogramowaniem i konfigurację systemu w technologii Group Policy.
Wsparcie techniczne	12 miesięcy

Załącznik nr 1.4 – Szczegółowy opis przedmiotu zamówienia (część 4)

Część 4 – Dostawa Pakietu oprogramowania biurowego (wersja edukacyjna) – 13 szt.

4.1 Pakiet oprogramowania biurowego (wersja edukacyjna) – 13 sztuk	
Opis	Najnowszy stabilny pakiet oprogramowania biurowe zawierające następujące elementy: procesor tekstu, arkusz kalkulacyjny, program do prezentacji, w pełni wspierający formaty plików .docx, .xlsx, .pptx, .accdb język polski zawierający aplikację służącą do obsługi poczty elektronicznej i organizacji czasu oraz umożliwiającą współpracę z serwerem przy pomocy protokołu dostępu MAPI/RPC. Zamawiający posiada edukacyjną grupową licencję oprogramowania Microsoft o numerze OPEN 98498763ZZE1911 lub równoważny spełniający powyższy opis.
Wsparcie techniczne	12 miesięcy

Załącznik nr 1.5 – Szczegółowy opis przedmiotu zamówienia (część 5)

Część 5 – Dostawa karty graficznej – 1 szt.

5.1 Karta graficzna – 1 sztuka	
Rodzaj złącza	PCI-E X16 3.0
Pamięć	3 GB DDR5
Szyna pamięci	192-bit
Taktowanie pamięci	8000 MHz
Taktowanie rdzenia	1500 MHz
Liczba rdzeni CUDA	1152
Rodzaje wyjść	HDMI - 1 szt. DP – 3 szt. DVI – 1 szt.
Chłodzenie	2 wentylatory
Gwarancja	24 miesiące

Załącznik nr 1.6 – Szczegółowy opis przedmiotu zamówienia (część 6)

Część 6 – Dostawa dysku wewnętrznego SSD 250 GB– 2 szt.

6.1 Dysk wewnętrzny SSD 250 GB – 2 sztuki	
Pojemność	250 GB
Format	2,5"
Interfejs	SATA 6 Gb/s
Prędkość odczytu	550 MB/s
Prędkość zapisu	520 MB/s
Odczyt losowy	98,000 IOPS
Zapis losowy	90,000 IOPS
MTBF (h)	1,500,000
Gwarancja	24 miesiące

Załącznik nr 1.7 – Szczegółowy opis przedmiotu zamówienia (część 7)

Część 7 – Dostawa pamięci RAM 4 GB – 1 szt.

7.1 Pamięć RAM – 1 sztuka	
Pojemność	4GB
Typ pamięci	DDR3
Częstotliwość	1600MHz
Inne	Pamięć RAM pozwalająca rozszerzyć funkcjonalność posiadanego komputera stacjonarnego lub równoważna pamięć RAM zgodna z powyższymi parametrami.
Gwarancja	24 miesiące

Załącznik nr 1.8 – Szczegółowy opis przedmiotu zamówienia (część 8)

Część 8 – Dostawa karty micro SD 256 GB – 10 szt.

8.1 Karta microSD 256 GB – 10 sztuk	
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:
Pojemność	256GB
Interfejs	USB 3.0
Prędkość odczytu	160 MB/s
Prędkość zapisu	90 MB/s
Gwarancja	36 miesięcy

Załącznik nr 1.9 – Szczegółowy opis przedmiotu zamówienia (część 9)

Część 9 – Dostawa dysku wewnętrznego 500 GB –1 szt.

9.1 Dysk wewnętrzny SSD 500 GB – 1 sztuka	
Zastosowanie	Dysk pasujący do laptopa ze złączem SSD M.2 PCIe
Pojemność	500 GB
Interfejs	PCI Express 3.0 x4 M.2
Prędkość odczytu	3500 MB/s
Prędkość zapisu	2500 MB/s
MTBF (h)	1 500 000
Gwarancja	36 miesięcy

Załącznik nr 1.10 – Szczegółowy opis przedmiotu zamówienia (część 10)

Część 10 – Dostawa pakietu bezpieczeństwa antywirusowego przeznaczonego do ochrony komputerów – licencja – 250 szt., pakietu ochrony skrzynek pocztowych – licencja – 200 szt., pakietu ochrony urządzeń mobilnych – licencja – 5 szt.

10.1 Oprogramowanie antywirusowe	
Nazwa	Opis minimalnych wymagań:
Wymagania użytkowe oprogramowania:	<p>Przedłużenie licencji programu posiadanego przez Zamawiającego na okres 36 miesięcy, składająca się z następujących pakietów:</p> <ol style="list-style-type: none"> 1.1. Ochrona stacji roboczych dla 250 stanowisk 1.2. Ochrona skrzynek pocztowych dla 200 użytkowników 1.3. Ochrona urządzeń mobilnych w ilości 5 sztuk <p>Przedłużenie licencji na kolejny wymagany okres ma nastąpić z dniem 31.03.2019 r.</p>
1.1 Pakiet bezpieczeństwa antywirusowego przeznaczony do ochrony komputerów	
Wymagania	<ol style="list-style-type: none"> 1. Licencja na oprogramowanie do ochrony stacji roboczych dla 250 stanowisk. 2. Pełne wsparcie dla systemu Windows Vista/Windows 7/Windows 8/Windows 8.1/Windows 8.1 Update/10 3. Wsparcie dla 32- i 64-bitowej wersji systemu Windows. 4. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim. 5. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. 6. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim. 7. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives
Ochrona antywirusowa i antyspyware	<ol style="list-style-type: none"> 1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 3. Wbudowana technologia do ochrony przed rootkitami. 4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 7. 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. 8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). 9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy



	<p>skrót w menu kontekstowym.</p> <ol style="list-style-type: none">10. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.11. Możliwość skanowania dysków sieciowych i dysków przenośnych.12. Skanowanie plików spakowanych i skompresowanych.13. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.14. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku ale również ma być możliwe użycie symbolu wieloznacznego „*” zastępującego dowolne znaki w ścieżce.15. Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik.16. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.17. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.18. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.19. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.20. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.21. 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.22. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).23. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.24. 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).25. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.26. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.27. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.28. 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.
29. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
 30. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
 31. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
 32. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
 33. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
 34. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
 35. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
 36. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
 37. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
 38. W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.
 39. 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.
 40. 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.
 41. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
 42. Możliwość wysłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
 43. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
 44. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu



	<p>kwarantanny do laboratorium producenta.</p> <p>45. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.</p> <p>46. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.</p> <p>47. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.</p> <p>48. 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.</p> <p>49. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykłe oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.</p> <p>50. 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.</p> <p>51. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.</p> <p>52. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.</p> <p>53. 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.</p> <p>54. 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.</p> <p>55. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły.</p> <p>56. 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.</p> <p>57. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.</p> <p>58. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.</p> <p>59. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby</p>
--	---

	<p>skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika</p> <p>60.Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).</p> <p>61.Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:</p> <ul style="list-style-type: none">• tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,• tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,• tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,• tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach.• Tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach. <p>62.Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.</p> <p>63.Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.</p> <p>64.Oprogramowanie musi posiadać zaawansowany skaner pamięci.</p> <p>65.Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytelnikach PDF, aplikacjach JAVA itp.</p> <p>66.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.</p> <p>67.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.</p> <p>68.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.</p> <p>69.Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.</p> <p>70.Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.</p> <p>71.Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.</p> <p>72.Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.</p>
--	--



	<p>73. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http</p> <p>74. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).</p> <p>75. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antyvirus, antyspyware, metody heurystyczne, zapora sieciowa).</p> <p>76. Program ma być w pełni zgodny z technologią CISCO Network Access Control.</p> <p>77. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.</p> <p>78. 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.</p> <p>79. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.</p> <p>80. 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.</p> <p>81. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.</p> <p>82. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.</p> <p>83. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.</p> <p>84. Możliwość podejrzenia licencji za pomocą, której program został aktywowany.</p> <p>85. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: ochrona antywirusowa i antyspyware, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, , Obsługa technologii Microsoft NAP.</p> <p>86. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.</p> <p>87. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.</p> <p>88. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas po którym automatycznie zostają przywrócone dotychczasowe ustawienia.</p> <p>89. Administrator ma możliwość wstrzymania polityk na 10 min, 30 min, 1 godzinę i 4 godziny</p> <p>90. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za</p>
--	---

	<p>pomocą hasła lub konta użytkownika.</p> <p>91. Program musi posiadać opcję automatycznego skanowania komputera po dokonaniu zmian z użyciem opcji wstrzymania polityki.</p> <p>92. Aplikacja musi posiadać funkcję ręcznej aktualizacji komponentów programu.</p> <p>93. 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.</p> <p>94. Program musi posiadać możliwość definiowania stanów aplikacji, jakie będą wyświetlane użytkownikowi np. powiadomień o wyłączonych mechanizmach ochrony czy stanie licencji.</p> <p>95. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.</p> <p>96. Program musi posiadać funkcjonalność skanera EFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>97. Wbudowany skaner EFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.</p> <p>98. Aplikacja musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.</p> <p>99. Administrator ma możliwość dodania wykluczenia na podstawie procesu, wskazującego bezpośrednio na określony plik wykonywalny.</p> <p>100. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania wybranej ścieżki, w której znajdują się pliki i foldery, które mają zostać wyłączone ze skanowania.</p> <p>101. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania obiektu co najmniej w oparciu o nazwę zagrożenia oraz jego lokalizację.</p> <p>102. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania pliku, wskazując sumę kontrolną pliku (jego HASH).</p> <p>103. Program musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”</p> <p>104. Program musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów.</p> <p>105. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.</p> <p>106. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.</p> <p>107. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.</p> <p>108. Administrator musi posiadać możliwość zastosowania reguł dla kontroli dostępu do stron w zależności od zdefiniowanego przedziału czasowego.</p>
--	---

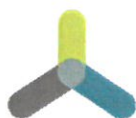
	<p>109. Program musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”</p> <p>110. Program musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów.</p> <p>111. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.</p> <p>112. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.</p> <p>113. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.</p> <p>114. Administrator musi posiadać możliwość zastosowania reguł dla kontroli dostępu do stron w zależności od zdefiniowanego przedziału czasowego.</p>
<p>Ochrona przed spamem</p>	<p>115. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.</p> <p>116. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.</p> <p>117. Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego.</p> <p>118. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.</p> <p>119. 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.</p> <p>120. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam.</p> <p>121. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam.</p> <p>122. Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci” obecnym w programie Microsoft Outlook.</p> <p>123. 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”.</p> <p>124. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.</p>
<p>Zapora osobista (personal firewall)</p>	<p>125. Zapora osobista ma pracować jednym z 4 trybów:</p> <ul style="list-style-type: none"> • tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora • tryb interaktywny – program pyta się o każde nowe nawiązywane

	<p>połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo),</p> <ul style="list-style-type: none">• tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany,• tryb uczenia się – umożliwi zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji. <p>126. Program musi akceptować istniejące reguły w zaporze systemu Windows, zezwalające na ruch przychodzący.</p> <p>127. Możliwość tworzenia list sieci zaufanych</p> <p>128. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie</p> <p>129. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.</p> <p>130. Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję.</p> <p>131. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń.</p> <p>132. Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.</p> <p>133. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.</p> <p>134. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.</p> <p>135. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.</p> <p>136. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.</p> <p>137. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.</p> <p>138. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.</p> <p>139. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci</p> <p>140. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.</p> <p>141. 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.</p> <p>142. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6</p> <p>143. Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem</p>
--	--



	<p>zwiększenia dokładności identyfikacji danej sieci.</p> <p>144. Program musi umożliwić ustalenie tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia.</p> <p>145. Program musi posiadać kreator, który umożliwi rozwiązać problemy z połączeniem. Musi on działać w oparciu o:</p> <ul style="list-style-type: none">• rozwiązanie problemów z aplikacją lokalną którą wskazujemy z listy.• rozwiązywanie problemów z połączeniem z urządzeniem zdalnym na podstawie adresu IP.
Kontrola dostępu do stron internetowych	<p>146. Aplikacja musi być wyposażony w zintegrowany moduł kontroli odwiedzanych stron internetowych.</p> <p>147. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.</p> <p>148. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.</p> <p>149. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.</p> <p>150. Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i pod kategorii.</p> <p>151. Podstawowe kategorie w jakie aplikacja musi być wyposażony 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.</p> <p>152. Moduł musi posiadać także możliwość grupowania kategorii już istniejących.</p> <p>153. Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta.</p> <p>154. Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.</p> <p>155. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj.</p> <p>156. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny.</p>
Administracja zdalna	<p>157. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2008 R2, 2012,2016 oraz systemach Linux.</p> <p>158. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).</p> <p>159. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.</p> <p>160. Konsola administracyjna musi umożliwiać podgląd szczegółów dotyczących bazy danych takich jak serwer Bazy danych, nazwę bazy danych, aktualny rozmiar bazy danych, nazwę hosta bazy danych</p> <p>161. Serwer administracyjny musi oferować możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych</p> <p>162. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika.</p>

163. Rozwiązanie ma być w pełni zgodne z rozporządzeniem RODO
164. 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.
165. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
166. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.
167. Konsola musi umożliwiać zarządzanie wszystkimi rozwiązaniami Producenta zabezpieczającymi przed zagrożeniami
168. Konsola musi umożliwiać zarządzanie systemem dynamicznej ochrony przed zagrożeniami
169. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
170. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.
171. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.
172. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
173. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
174. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
175. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie „hardware fingerprint”
176. Serwer administracyjny musi oferować natywne wsparcie dla „VDI” oraz „Golden Master Image”
177. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci.
178. Instalacja serwera administracyjnego powinna oferować możliwość pracy w sieci rozproszonej nie wymagając dodatkowego serwera proxy.
179. Rozwiązanie ma oferować możliwość komunikacji agenta przy wykorzystaniu http Proxy wbudowanego w serwer centralnego zarządzania bez wykorzystania dodatkowej maszyny Proxy
180. Serwer musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.
181. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
182. Serwer administracyjny musi oferować możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS
183. Serwer administracyjny musi oferować możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP
184. Serwer administracyjny musi oferować możliwość konfiguracji polityk zabezpieczeń takich jak ograniczenia funkcjonalności urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11
185. Serwer administracyjny musi oferować możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Map Google
186. 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.
187. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów.
 188. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
 189. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
 190. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows.
 191. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
 192. Centralna administracja musi pozwalać na zarządzanie urządzeniami mobilnymi z systemem iOS
 193. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
 194. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
 195. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
 196. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej.
 197. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów bazowych zarządzanego komputera oraz weryfikację zainstalowanego oprogramowania firm trzecich na stacji dla systemów Windows, Mac oraz Linux z możliwością jego odinstalowania
 198. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
 199. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego.
 200. Konsola ma oferować możliwość aktywacji oraz wdrożenie elementów systemu EDR producenta.
 201. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny.
 202. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
 203. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
 204. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
 205. Serwer administracyjny musi oferować możliwość zablokowania,



- odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzeniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.
206. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.
207. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
208. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
209. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
210. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
211. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
212. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
213. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
214. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego.
215. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
216. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.
217. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.
218. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
219. 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.
220. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji.
221. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
222. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.
223. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas



	<p>instalacji nowego pakietu.</p> <p>224. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.</p> <p>225. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.</p> <p>226. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.</p> <p>227. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.</p> <p>228. Serwer administracyjny musi oferować możliwość utworzenia grup dynamicznych na podstawie zainstalowanego oprogramowania oraz zainstalowanych podzespołów bazowych w komputerach końcowych.</p> <p>229. 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, podzespoły bazy itp.</p> <p>230. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.</p> <p>231. 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.</p> <p>232. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.</p> <p>233. 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.</p> <p>234. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.</p> <p>235. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta</p> <p>236. Serwer administracyjny musi posiadać minimum 40 szablonów raportów przygotowanych przez producenta</p> <p>237. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.</p> <p>238. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.</p> <p>239. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.</p> <p>240. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp.</p>
--	--



241. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania oraz zapisania szablonów stworzonych filtrów
242. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
243. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostęp do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów.
244. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.
245. Serwer administracyjny musi oferować możliwość wygenerowania raportu na podstawie danych z systemu EDR producenta
246. Serwer administracyjny musi oferować możliwość wygenerowania raportu na podstawie informacji o zainstalowanych podzespołach w stacjach roboczych
247. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.
248. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie.
249. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.
250. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
251. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
252. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.
253. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień na zasadzie „WYSIWYG” z wykorzystaniem istniejących zmiennych
254. Powiadomienia mailowe mają być wysyłane w formacie HTML
255. Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania.
256. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
257. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
258. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
259. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.

260. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji bądź korzystając z powiązanego konta systemu zarządzania licencjami.
261. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
262. W przypadku posiadania tylko jednej dodanej licencji do konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania
263. Rozwiązanie ma oferować weryfikacji zainstalowanych komponentów bazowych urządzenia takich jak: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe, etc
264. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
265. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia.
266. Serwer administracyjny musi być wyposażony w mechanizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.
267. W przypadku wystąpienia problemu rozwiązanie ma oferować możliwość przekierowania do wyszukiwarki Google z odwołaniem do konkretnego kodu błędu, który wystąpił w środowisku
268. Serwer administracyjny oferować łatwy dostęp do zadań z poziomu menu kontekstowego w zależności od rodzaju urządzenia.
269. Serwer administracyjny musi oferować aktualizację wszystkich komponentów z poziomu raportów jednym kliknięciem.
270. Serwer administracyjny musi oferować możliwość konfiguracji listy adresów multicast
271. Serwer administracyjny musi oferować WOL przy wykorzystaniu multicast
272. Rozwiązanie ma oferować instalację agenta rozwiązania DLP producenta z poziomu jednego repozytorium.
273. 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.
274. Konfiguracja zestawów uprawnień musi umożliwiać przypisanie praw tylko do odczytu, odczytu i użycia, oraz prawo do zapisania zmian w ramach danego zadania lub polityki w konsoli ERA.
275. Rozwiązanie ma oferować zebrania logu diagnostycznego którego pobranie będzie możliwe z poziomu konsoli WEB
276. Logi diagnostyczny, który można pobrać bezpośrednio z konsoli z modułów Anty SPM, firewall, HIPS, kontroli dostępu do urządzeń, kontroli dostępu do stron internetowych
277. Logi diagnostyczne do pobrania z poziomu konsoli mają być dostępne 24h od daty ich wygenerowania



	<p>278. Konsola webowa musi umożliwiać stronicowanie w widoku komputerów w celu ograniczenia liczby wyświetlanych maszyn na jednej stronie</p> <p>279. Konsola webowa musi umożliwiać weryfikację plików wysyłanych do serwerów producenta</p> <p>280. Konsola webowa musi umożliwiać zarządzanie systemem EDR producenta.</p> <p>281. Administrator musi mieć możliwość podłączenia do stacji roboczej z użyciem protokołu RDP bezpośrednio z poziomu konsoli ERA.</p> <p>282. Konsola administracyjna musi oferować możliwość weryfikacji zmian w produktach wprowadzanych przez producenta (Release notes dostępne bezpośrednio z konsoli zarządzania)</p> <p>283. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar</p> <p>284. Musi istnieć mechanizm, umożliwiający dodawanie reguł do istniejących już w module firewalla lub harmonogramie. Takie reguły można umieścić na początku lub końcu istniejącej listy.</p> <p>285. Administrator musi otrzymywać powiadomienia o dostępnych aktualizacjach z poziomu interfejsu Konsoli administracyjnej</p> <p>286. Konsola administracyjna musi umożliwiać dodanie własnego logotypu do interfejsu webowego.</p>
10.2. Ochrona skrzynek pocztowych	
Wymagania	<ol style="list-style-type: none">1. Licencja na oprogramowanie do ochrony skrzynek pocztowych dla 200 użytkowników2. Skaner antywirusowy, antyspyware3. Możliwość skanowania wszystkimi modułami programu (heurystyka, sygnatury, adware/spyware, aplikacje niepożądane, aplikacje niebezpieczne)4. Skanowanie plików, plików spakowanych, archiwów samorozpakowujących, plików wiadomości e-mail5. Konfiguracja wszystkich modułów oprogramowania (z wyjątkiem konfiguracji systemu antyspamowego) ma być możliwa poprzez edycję jednego pliku konfiguracyjnego6. Możliwość ustawień limitów dla modułu skanującego względem maksymalnego rozmiaru pliku, maksymalnej liczby warstw kompresji, maksymalnego rozmiaru archiwum, maksymalnego czasu skanowania, maksymalnego rozmiaru archiwum samorozpakowującego, rozszerzenia skanowanego pliku7. Możliwość tworzenia kwarantanny dla plików zainfekowanych w dowolnej lokalizacji w systemie plików8. Możliwość zdefiniowania częstotliwości aktualizacji programu z dokładnością do jednej minuty osobno dla aktualizacji sygnatur oraz osobno dla aktualizacji systemu antyspamowego9. Brak potrzeby instalacji dodatkowych zależności do systemu oprócz biblioteki LIBC, oprogramowanie po instalacji jest od razu gotowe do pracy10. Wbudowany bezpośrednio w program system obsługi plików spakowanych niewymagający zewnętrznych komponentów zainstalowanych w systemie11. Brak potrzeby instalacji źródeł jądra systemu oraz kompilacji jakichkolwiek modułów jądra do skanowania plików na żądanie12. Możliwość tworzenia przynajmniej pięciu poziomów dokładności czyszczenia zainfekowanych plików13. Możliwość zdefiniowania liczby wątków oraz liczby procesów dla każdego z modułów skanujących14. Możliwość tworzenia różnych akcji (przynajmniej 5-ciu różnych) w zależności



	<p>od typu zdarzenia (w przypadku pliku nie przeskanowanego, pliku przeskanowanego, pliku zainfekowanego).</p> <ol style="list-style-type: none">15. Logowanie wykonanych akcji na plikach oraz zdarzeń dla poszczególnych modułów oprogramowania16. Wsparcie dla zewnętrznego serwera logującego syslog, możliwość definiowania dowolnego pliku logu (np. daemon, mail, user itp.)17. Możliwość zdefiniowania przynajmniej sześciu poziomów logowania programu18. Możliwość uruchomienia interfejsu programu dostępnego przez przeglądarkę Web19. Interfejs ma umożliwiać modyfikację ustawień programu oraz jego aktualizację a także przegląd statystyk dotychczas przeskanowanych plików20. Interfejs programu dostępny przez przeglądarkę Web wykorzystuje wbudowany w program serwer http21. Możliwość uruchomienia interfejsu Web na dowolnym porcie TCP22. Możliwość uruchomienia interfejsu Web na dowolnym interfejsie sieciowym23. Możliwość zabezpieczenia dostępu do interfejsu Web poprzez zdefiniowanie nazwy użytkownika i hasła24. Interfejs Web ma przedstawić administratorowi dokładny wynik skanowania poszczególnych plików w systemie wraz z możliwością pobrania tych wyników w postaci pliku tekstowego celem późniejszej analizy25. Możliwość podglądu informacji o licencji bezpośrednio z poziomu interfejsu Web, która zawiera przynajmniej informacje o liczbie dni do wygaśnięcia licencji, nazwę użytkownika licencji oraz pełną nazwę produktu, którego dotyczy licencja26. Program ma być wyposażony w graficzny menadżer kwarantanny dostępny z poziomu interfejsu Web. Menadżer ma oferować administratorowi możliwość przeglądu, pobrania, dodania i usunięcia plików w kwarantannie27. Menadżer kwarantanny ma posiadać możliwość wyszukiwania plików znajdujących się w kwarantannie przynajmniej po nazwie pliku, dodania pliku (możliwość definiowania przedziałów czasowych), rozmiarze (możliwość definiowania minimalnej i maksymalnej wielkości) oraz ilości plików (możliwość definiowania minimalnej i maksymalnej ilości)28. Interfejs Web do zarządzania produktem ma opierać się o wbudowane w program biblioteki PHP w wersji nie niższej niż 5.2.829. Interfejs dostępny poprzez przeglądarkę Web ma umożliwiać zarządzanie programem również wtedy, gdy przeglądarka nie obsługuje kodu JavaScript30. Możliwość stworzenia lokalnego repozytorium aktualizacji dla przynajmniej dwóch różnych produktów antywirusowych instalowanych na stacjach Windows31. Możliwość definicji użytkownika systemowego z prawami, którego zostanie uruchomiony demon skanujący32. Współpraca z mechanizmem automatycznej wysyłki podejrzanych plików do laboratorium producenta33. Wysyłka podejrzanych plików ma być możliwa bezpośrednio do producenta lub za pośrednictwem serwera zdalnego zarządzania34. Możliwość uaktywnienia dodatkowych funkcjonalności programu (moduł skanujący dla bramek sieciowych oraz moduł skanujący system plików), które nie wymagają od użytkownika instalacji dodatkowych zależności ani modułów a jedynie zacytowanie dodatkowych plików licencji
--	--

	<p>35. Możliwość instalacji na dowolnym systemie Linux 2.6.x i nowszym.</p> <p>36. Producent ma dostarczyć pakiety instalacyjne w formacie RPM (dla dystrybucji Red Hat Mandriva, Suse oraz innych z nimi zgodnych), DEB (dla dystrybucji Debian, Ubuntu oraz innych z nimi zgodnych) oraz archiwum TGZ dla wszystkich pozostałych</p> <p>37. Możliwość instalacji na systemie FreeBSD 6.x, 7.x, 8.x i 9.x</p> <p>38. Wsparcie dla platform 32 oraz 64 bitowych</p> <p>39. Architektura programu umożliwia jego uruchomienie i optymalizację zarówno dla systemów jedno jak i wieloprocesorowych</p> <p>40. System ma mieć możliwość powiadomienia administratora o wykryciu infekcji oraz powiadomienia o zbliżającym się terminie wygaśnięcia licencji za pośrednictwem poczty e-mail.</p> <p>41. Możliwość szybkiej konfiguracji oprogramowania poprzez skrypt powłoki. Skrypt umożliwia prostą konfigurację oprogramowania stosownie do wykrytego systemu operacyjnego, w jakim oprogramowanie zostało zainstalowane.</p> <p>42. Skrypt ma mieć możliwość konfiguracji reguł firewalla w taki sposób, aby przekierować niezbędne usługi do poszczególnych modułów programu.</p> <p>43. Skrypt konfiguracyjny dla powłoki systemu ma zawierać funkcję przywrócenia wprowadzonych zmian regułach firewalla</p> <p>44. Możliwość skanowania ruchu SMTP, POP3, IMAP</p> <p>45. Możliwość integracji z popularnymi systemami pocztowymi w tym przynajmniej z MTA Sendmail, Postfix, Exim, Qmail, Zmailer i CommuniGate Pro</p> <p>46. Integracja z MTA ma zapewniać obustronne skanowanie ruchu pocztowego (ruchu przychodzącego oraz wychodzącego)</p> <p>47. Możliwość integracji z dowolnym systemem MDA celem skanowania wyłącznie poczty przychodzącej do serwera</p> <p>48. Możliwość pracy w trybie proxy SMTP celem skanowania wyłącznie poczty wychodzącej z serwera</p> <p>49. Możliwość pracy w trybie proxy POP3 celem skanowania poczty pobieranej przez użytkowników z serwera POP3</p> <p>50. Możliwość pracy w trybie proxy IMAP celem skanowania poczty pobieranej przez użytkowników z serwera IMAP</p> <p>51. Możliwość współpracy z systemem AmaViS</p> <p>52. Możliwość tworzenia różnych profili konfiguracji w zależności od adresu e-mail lub domeny osobno dla nadawców lub odbiorców wiadomości</p> <p>53. Możliwość tworzenia białych i czarnych list domen i adresów e-mail</p> <p>54. Wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty</p> <p>55. Konfiguracja filtra antyspamowego ma znajdować się w innym pliku konfiguracyjnym niż konfiguracja skanera antywirusowego</p> <p>56. Producent programu ma wyposażyć program w przynajmniej 5 predefiniowanych profili systemu antyspamowego</p> <p>57. System antyspamowy ma być wyposażony przynajmniej sprawdzanie list RBL oraz mechanizm reputacji poczty.</p> <p>58. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.</p>
<p>10.3. Ochrona urządzeń mobilnych</p>	
<p>Wymagania</p>	<p>1. Licencja na oprogramowanie do ochrony urządzeń mobilnych w ilości</p>

	<p>5 sztuk</p> <ol style="list-style-type: none"> 2. Wspierany system co najmniej Android 4.0 (Ice Cream Sandwich) 3. Rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa. 4. Procesor: ARM (minimum ARMv7) 5. Pamięć wewnętrzna: 20 MB. 6. Połączenie z siecią Internet dla celów aktualizacji sygnatur i aktywacji licencji <p>Ochrona antywirusowa:</p> <ol style="list-style-type: none"> 7. Ochrona plików w czasie rzeczywistym 8. Ochrona przed atakami typu „phishing” 9. Skanowanie rozszerzeń DEX, bibliotek SO plików archiwum oraz innych. 10. Skanowanie dostępnego w urządzeniu nośnika pamięci SD. 11. Aplikacja musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne 12. Ochrona proaktywna wykrywająca nieznanne zagrożenia. 13. Aplikacja ma mieć możliwość określenia poziomu głębokości skanowania plików archiwum. 14. Aplikacja ma mieć możliwość określenia domyślnej akcji podejmowanej w przypadku wykrycia zagrożenia: przeniesienia do kwarantanny, usunięcia lub zignorowania. 15. W przypadku wykrycia zagrożenia użytkownik ma otrzymać odpowiednie powiadomienie 16. Aplikacja musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia 17. Aplikacja musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności, w pełni naładowane i podłączone do ładowarki <p>Skanowanie na żądanie:</p> <ol style="list-style-type: none"> 18. Aplikacja ma mieć możliwość skanowania zainstalowanych aplikacji. 19. Aplikacja ma wykorzystywać do celu skanowania metody heurystyczne wykrywające nieznanne zagrożenia. 20. Informacje o skanowaniu mają być przechowywane w plikach dziennika. 21. Użytkownik ma mieć możliwość wskazania akcji jaka ma być podjęta w przypadku wykrycia zagrożenia: poddania kwarantannie, usunięcia lub zignorowania. 22. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia, lub wskazania folderu, który ma być przeskanowany. 23. Aplikacja ma posiadać osobne dzienniki skanowania dla ochrony plików w czasie rzeczywistym, oraz skanowania na żądanie. <p>Filtr SMS/MMS i połączeń (jeśli system zezwala): Użytkownik musi mieć możliwość definiowania własnych reguł dotyczących połączeń oraz wiadomości SMS/MMS bez konieczności podawania hasła administratora</p> <ol style="list-style-type: none"> 24. Reguły zdefiniowane przez administratora (w trybie administratora) muszą mieć wyższy priorytet niż reguły zdefiniowane przez użytkownika.
--	---

25. Użytkownik i administrator ma mieć możliwość tworzenia białej i czarnej listy numerów telefonów.
26. Użytkownik i administrator ma mieć możliwość dodania numeru telefonu, dla którego można określić akcje dla:
 - a. Przychodzącej wiadomości SMS
 - b. Przychodzącej wiadomości MMS
 - c. Połączenia wychodzącego
 - d. Połączenia przychodzącego.
27. Aplikacja ma mieć możliwość aktywacji blokady dla wszystkich połączeń oraz wiadomości SMS/MMS dla znanych kontaktów znajdujących się w książce telefonicznej urządzenia.
28. Aplikacja ma mieć możliwość blokady połączeń telefonicznych oraz wiadomości SMS/MMS dla nieznanymi kontaktów (nieznanymi znajdujących się w książce telefonicznej urządzenia).
29. Aplikacja ma mieć możliwość blokowania anonimowych połączeń przychodzących (pochodzących z ukrytych ID).
30. Aplikacja ma być wyposażona w dziennik modułu antyspamowego zawierający informacje odnośnie filtrowania modułu.

Ochrona przed kradzieżą:

31. Użytkownik ma mieć możliwość wprowadzenia zaufanej karty SIM.
32. Dodanie zaufanej karty SIM ma się odbyć się w oparciu o kartę wprowadzoną w danym urządzeniu lub w oparciu o dane wprowadzone ręcznie.
33. Wprowadzenie danych ręcznie dotyczących zaufanej karty SIM ma się odbywać w oparciu o numer IMSI karty SIM.
34. Aplikacja ma mieć możliwość wprowadzenia zaufanych odbiorców wiadomości, do których zostanie przesłana informacja w przypadku umieszczenia w urządzeniu innej niż zaufana karty SIM.
35. Aplikacja ma mieć możliwość włączenia opcji ignorowania niedopasowania kart SIM.
36. Użytkownik ma mieć możliwość edycji treści wiadomości SMS wysyłanej na zaufane numery telefonów w przypadku nie dopasowania karty SIM.
37. W przypadku kradzieży urządzenia, prawowity użytkownik ma mieć możliwość wysłania na urządzenie komendy która umożliwi:
 - a. usunięcie zawartości urządzenia
 - b. zablokowania urządzenia
 - c. przesłania na zaufany numer telefonu lokalizacji GPS w której skradzione urządzenie się znajduje.
38. Administrator musi mieć możliwość wysyłania powyższych komend bezpośrednio z poziomu konsoli centralnego zarządzania
39. Możliwość zdalnego zresetowania hasła ma być możliwa tylko w przypadku wysłania odpowiedniego polecenia z zaufanego urządzenia

Polityka ustawień:

Aplikacja musi posiadać funkcjonalność pozwalającą administratorowi na monitorowanie ustawień urządzenia w celu weryfikacji czy są one zgodne z polityką.

40. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia:



- a. Połączenie Wi-Fi
 - b. Satelity GPS
 - c. Usługi lokalizacyjne
 - d. Pamięć
 - e. Roaming danych
 - f. Roaming połączeń
 - g. Nieznane źródła
 - h. Tryb debugowania
 - i. Komunikacja NFC
 - j. Szyfrowanie pamięci masowej
41. Administrator ma mieć możliwość wyboru powyższych elementów

Kontrola aplikacji:

42. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji
43. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji
44. Blokowanie aplikacji musi być umożliwione co najmniej za pomocą polityk:
- a. manualnego zdefiniowania listy blokowanych aplikacji na podstawie nazwy
 - b. blokowanie na podstawie kategorii (np. kategorii Gry lub Społecznościowe)
 - c. blokowanie na podstawie uprawnień aplikacji (np. aplikacji, które korzystają z modułu GPS do odczytania lokalizacji)
 - d. blokowanie na podstawie źródła (np. aplikacje instalowane z innych źródeł niż sklep Google Play)
45. Administrator musi mieć możliwość monitorowania czasu, jaki użytkownik spędza na korzystaniu z poszczególnych aplikacji i sprawdzenia z jakich aplikacji użytkownik korzystał w ciągu ostatnich 30 dni, 7 dni oraz 24 godzin.

Zabezpieczenia urządzenia:

46. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej:
- a. minimalny poziom zabezpieczeń i złożoność blokady ekranu
 - b. maksymalną dopuszczaną liczbę błędnych prób odblokowania
 - c. odstęp czasu po którym użytkownik musi zmienić kod odblokowujący urządzenie
 - d. czas przeznaczony na odblokowanie urządzenia
 - e. ograniczyć dostęp do kamery wbudowanej w urządzenie

Aktualizacje sygnatur:

47. Wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.
48. Aplikacja ma mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje sygnatur co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin.
49. Aplikacja ma mieć funkcjonalność ochrony hasłem wybranych

	<p>modułów ochrony, w tym co najmniej dostępu do ustawień ochrony antywirusowej, ustawień modułu antyspamowego, ochrony przed kradzieżą, uruchamiania zadań audytu zabezpieczeń oraz przed deinstalacją.</p> <p>50. Aplikacja ma mieć możliwość ukrycia ikony powiadomień.</p> <p>Konfiguracja i zdalne zarządzanie:</p> <p>51. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne</p> <p>52. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją</p> <p>53. Administrator musi mieć możliwość zdalnego wysyłania komunikatów z poziomu konsoli centralnego zarządzania do użytkowników urządzeń mobilnych</p> <p>54. Przesłana wiadomość musi wyświetlać się w formie wyskakującego okna, aby użytkownik ich nie przeoczył</p> <p>55. Administrator musi mieć możliwość kontrolowania mechanizmu aktualizacji oprogramowania</p>
--	---

Załącznik nr 1.11 – Szczegółowy opis przedmiotu zamówienia (część 11)

Część 11 – Dostawa komputerów stacjonarnych – 4 szt.

11.1 Komputer biurowy z system operacyjnym - 4 sztuki	
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:
Typ	Komputer stacjonarny wykonany przez jednego producenta. W ofercie wymagane jest podanie modelu, symbolu oraz producenta podzespołów komputera
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb przetwarzania aplikacji biurowych, aplikacji edukacyjnych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych.
Wydajność obliczeniowa	Procesor taktowany zegarem co najmniej 2,8 GHz, pamięci cache 9 MB lub równoważny procesor klasy x86 zapewniający spełnienie poniższych kryteriów wydajności: - wydajność całego oferowanego systemu komputerowego min. 1115 pkt w teście BAPCo SYSMark 2014 . Test SYSMark 2014 Results powinien być wykonany w konfiguracji całego komputera identycznej z wymaganą oraz przy rozdzielczości ekranu co najmniej 1920 x 1080 pikseli i innymi ustawieniami zgodnymi z zaleceniami producenta testu.
Pamięć operacyjna	8GB 2400 MHz możliwość rozbudowy do min 32 GB
Parametry pamięci masowej	Zbudowana w oparciu o pamięć flash co najmniej 500 GB SSD
Wydajność grafiki	Grafika zintegrowana z procesorem powinna umożliwiać pracę na 2 monitorach ze wsparciem dla DirectX 12, Open CL 2.0, OpenGL 4.4 – z możliwością dynamicznego przydzielenia pamięci 1,7 GB.
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, porty słuchawek i mikrofonu na przednim oraz na tylnym panelu obudowy
Obudowa	Miejsca na wewnętrzne dyski/napędy: 2 x 3,5", 1 x 2,5", Miejsca na zewnętrzne dyski/napędy: 1 x 3,5" 2 x 5,25", Wyprowadzone złącza Wejście mikrofonowe - 1 szt., Wyjście słuchawkowe/głośnikowe - 1 szt., USB 3.0 - 2 szt., USB 2.0 - 2 szt. Zasilacz o mocy minimum 210 W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85%, przy 50% obciążeniu.
Ergonomia	Suma wymiarów obudowy (wysokość + szerokość + głębokość mierzona po krawędziach zewnętrznych) nie może wynosić więcej niż 860 mm

Wymagania dodatkowe	Licencja najnowszego systemu operacyjnego. Stabilny system operacyjny w języku polskim, w pełni obsługujący pracę w domenie i kontrolę użytkowników w technologii ActiveDirectory, zcentralizowane zarządzanie poprogramowaniem i konfiguracją systemu w technologii Group Policy. System operacyjny, zainstalowany na sprzęcie komputerowym objętym przedmiotem zamówienia. Dołączony nośnik z oprogramowaniem, sterownikami, płyty Recovery umożliwiające instalacje systemu w wersji 64 bitowej.
interfejs	<p>Wbudowane porty i złącza w płyci głównej: Wbudowane porty minimalnie:</p> <ul style="list-style-type: none"> - 1 x DVI - 1 x DP - 1 x RJ-45 - 1 x PCI-E 3.0 16x - 2 x PCI-E 1x - 6.x USB 2.0 - 4x Złącza USB 3.0 <p>Dodatkowe informacje o portach USB 2.0/3.0/3.1</p> <ul style="list-style-type: none"> - 2 x USB 3.0 (przedni panel) - 2 x USB 3.0 (tylny panel) - 2 x USB 2.0 (przedni panel) - 2 x USB 2.0 (tylny panel) - 2 x USB 2.0 (wewnątrz) - 3 x Serial ATA
Poziom hałasu	W tryb pracy: 50% obciążenie procesora - 22 dB (osoba obsługująca)
Wymagania dodatkowe	Nagrywarka DVD +/-RW, klawiatura, mysz
Gwarancja komputera	24 miesiące producenta

Załącznik nr 1.12 – Szczegółowy opis przedmiotu zamówienia (część 12)

Część 12 – Dostawa monitorów 24 cale – 5 szt.

12.1 Monitor 24 cale – 5 sztuk	
Typ ekranu	Płasko ekranowy monitor panoramiczny LED, IPS 24”, przeciwoodblaskowa powłoka (matowa)
Jasność	300 cd/m ²
Kontrast	1000 :1 (typowy) 2 000 000 :1 (dynamiczny)
Wielkość plamki	0,27 mm
Kąty widzenia (pion/poziom)	178°/178°
Czas reakcji matrycy	8 ms
Kolory	16.7mln
Rozdzielczość maksymalna	1920 x 1200
Ustawienia ekranu w pionie i poziomie	Pivot
Złącze	VGA – 1 szt., DVI-D - 1 szt., Display Port - 1 szt., USB 2.0 – 4 szt.
Średnie użycie energii	Pobór prądu w trybie uśpienia-poniżej 0,5 W
Podstawa	kompatybilność z VESA 100mm
Normy i standardy	Monitory muszą być wykonane zgodnie normami i posiadać Certyfikaty: TCO 5.0, EPEAT Gold, Energy Star 5.1
Gwarancja	36 miesięcy

Załącznik nr 1.13 – Szczegółowy opis przedmiotu zamówienia (część 13)

Część 13 – Dostawa listwy głośnikowej dedykowanej do monitora – 5 szt.

13.1 Listwa głośnikowa dedykowana do monitora – 5 sztuk	
Zastosowanie	Oryginalne głośniki tego samego producenta co monitory posiadane przez Zamawiającego. Modele posiadanych monitorów to 2412M. Głośnik wyposażony jest w odpowiednie uchwyty.
Moc	2 x 5 W na kanał
Gniazda słuchawkowe	2 szt.
Zasilanie	12 V prądu stałego
Gwarancja	12 miesięcy



Załącznik nr 1.14 – Szczegółowy opis przedmiotu zamówienia (część 14)

Część 14 – Dostawa zestawów „klawiatura i mysz bezprzewodowa” – 7 szt.

14.1 Zestaw klawiatura i mysz bezprzewodowa – 7 sztuk	
Łączność	bezprzewodowa
Interfejs	2,4 GHz, USB (nanoodbiornik)
Klawiatura	Klawisze - cicha praca, mały skok, multimedialne, funkcyjne, podpórka pod nadgarstki, wyłącznik na przednim panelu klawiatury.
Mysz	Sensor – optyczny, 3 przyciski, rolka przewijania, rozdzielczość-1000dpi
Technologia czujnika:	Zaawansowane śledzenie optyczne
Gwarancja	24 miesiące

Załącznik nr 2 do SIWZ

.....
(pieczęć wykonawcy)

**Instytut Agrofizyki im. B. Dobrzańskiego
Polskiej Akademii Nauk
ul. Doświadczalna 4, 20-290 Lublin**

OFERTA WYKONAWCY

Odpowiadając na publiczne ogłoszenie o zamówieniu i w nawiązaniu do Specyfikacji Istotnych Warunków Zamówienia (SIWZ) z dnia 28 lutego 2019 r. w postępowaniu o zamówienie publiczne (znak: A-2401-9/2019) na **dostawę laptopów z oprogramowaniem, licencji oraz akcesoriów komputerowych dla Instytutu Agrofizyki im. B. Dobrzańskiego Polskiej Akademii Nauk w Lublinie z podziałem na 14 części**, składamy ofertę o treści odpowiadającej treści SIWZ:

WYKONAWCA:

Lp.	Nazwa(y) Wykonawcy(ów)	NIP	REGON	Adres(y) Wykonawcy(ów)	Numer tel i faksu, adres e:mailowy
1.					
2.					

Oferujemy wykonanie zamówienia zgodnie z przedmiotem zamówienia i wymaganiami określonymi w siwz – za cenę :

Część 1 – Dostawa komputerów PC laptopów – 9 szt.

a) Cena oferty

Lp.	Zamawiany przedmiot	Oferowany przedmiot	Ilość [szt]	Cena jednostkowa netto [PLN]*	Wartość netto [PLN]*	Stawka podatku VAT (%)*	Wartość podatku VAT [PLN]*	Wartość brutto [PLN]*
A	B	C	D	E	$F = D \times E$	G	$H = F \times G$	$I = F + H$

1	Komputer PC laptop- 9 szt.	1) Nazwa:*..... 2) Model*..... 3) Producent *..... 4) Kraj i rok produkcji *.....	9					
2	ŁĄCZNIE		---	---		---		

(CENA OFERTY BRUTTO tj. WARTOŚĆ BRUTTO OFERTY, zwana również wartością ceny całkowitej - stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w SIWZ)

W pozycjach nr: *..... ww. tabeli obowiązek podatkowy, zgodnie z przepisami o podatku od towarów i usług, leży po stronie Zamawiającego – (***Wypełnić jeśli dotyczy**)

b) Termin dostawy:

Oferujemy dostarczenie przedmiotu zamówienia w terminie nie przekraczającym:
.....* dni od dnia podpisania umowy.

UWAGA!!!

***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin realizacji stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

c) Termin gwarancji:

OKREŚLENIE TERMINU GWARANCJI	<u>TAK/NIE*</u>
Wykonawca rozszerza gwarancję z 12 miesięcy na 24 miesiące.	

UWAGA!!!

***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin gwarancji stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

Część 2 – Dostawa licencji na uaktualnienie systemu operacyjnego do wersji profesjonalnej (wersja edukacyjna)– 8 szt.,

a) Cena oferty

Lp.	Zamawiany przedmiot	Oferowany przedmiot	Ilość [szt]	Cena jednostkowa netto [PLN]*	Wartość netto [PLN]*	Stawka podatku VAT (%)*	Wartość podatku VAT [PLN]*	Wartość brutto [PLN]*
A	B	C	D	E	F= D x E	G	H = F x G	I = F + H
1	Licencja – 8 szt.	1) Nazwa:*..... 2) Producent *..... 3) Typ licencji*.....	8					
2	ŁĄCZNIE		---	---		---		

(CENA OFERTY BRUTTO tj. WARTOŚĆ BRUTTO OFERTY, zwana również wartością ceny całkowitej - stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w SIWZ)

W pozycjach nr: *..... ww. tabeli obowiązków podatkowych, zgodnie z przepisami o podatku od towarów i usług, leży po stronie Zamawiającego – (***Wypełnić jeśli dotyczy**)

b) Termin dostawy:

Oferujemy dostarczenie przedmiotu zamówienia w terminie nie przekraczającym:* dni od dnia podpisania umowy.

UWAGA!!!

***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin realizacji stanowi kryterium oceny ofert i będzie podlegał ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

c) Termin rozszerzenia wsparcia technicznego:

OKREŚLENIE ROZSZERZENIA WSPARCIA TECHNICZNEGO	TAK/NIE*
Wykonawca rozszerza wsparcie techniczne z 12 miesięcy na 24 miesiące.	

UWAGA!!!

***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: wsparcie techniczne stanowi kryterium oceny ofert i będzie podlegał ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

Część 3 – Dostawa licencji na uaktualnienie systemu operacyjnego do wersji profesjonalnej EN (wersja edukacyjna)– 1 szt.

a) Cena oferty

Lp.	Zamawiany przedmiot	Oferowany przedmiot	Ilość [szt]	Cena jednostkowa netto [PLN]*	Wartość netto [PLN]*	Stawka podatku VAT (%)*	Wartość podatku VAT [PLN]*	Wartość brutto [PLN]*
A	B	C	D	E	$F = D \times E$	G	$H = F \times G$	$I = F + H$
1	Licencja – 1 szt.	1) Nazwa:* 2) Producent *..... 3) Typ licencji*	1					
2	ŁĄCZNIE		---	---		---		

(CENA OFERTY BRUTTO tj. WARTOŚĆ BRUTTO OFERTY, zwana również wartością ceny całkowitej - stanowi kryterium oceny ofert i będzie podlegał ocenie zgodnie z zasadami opisanymi w SIWZ)

W pozycjach nr: *..... ww. tabeli obowiązków podatkowych, zgodnie z przepisami o podatku od towarów i usług, leży po stronie Zamawiającego – (***Wypełnić jeśli dotyczy**)

b) Termin dostawy:

Oferujemy dostarczenie przedmiotu zamówienia w terminie nie przekraczającym:* dni od dnia podpisania umowy.

UWAGA!!!

***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin realizacji stanowi kryterium oceny ofert i będzie podlegał ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

w rozdziale XIII SIWZ)

c) Termin rozszerzenia wsparcia technicznego:

OKREŚLENIE ROZSZERZENIA WSPARCIA TECHNICZNEGO	<u>TAK/NIE*</u>
Wykonawca rozszerza wsparcie techniczne z 12 miesięcy na 24 miesiące.	

UWAGA!!!
*NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ
(UWAGA: wsparcie techniczne stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

Część 4 – Dostawa Pakietu oprogramowania biurowego (wersja edukacyjna) – 13 szt.

a) Cena oferty

Lp.	Zamawiany przedmiot	Oferowany przedmiot	Ilość [szt]	Cena jednostkowa netto [PLN]*	Wartość netto [PLN]*	Stawka podatku VAT (%)*	Wartość podatku VAT [PLN]*	Wartość brutto [PLN]*
A	B	C	D	E	$F = D \times E$	G	$H = F \times G$	$I = F + H$
1	Pakiet oprogramowania –13 szt.	1) Nazwa:*..... 2) Producent *..... 3) Typ oprogramowania*	13					
2	ŁĄCZNIE		---	---		---		

(CENA OFERTY BRUTTO tj. WARTOŚĆ BRUTTO OFERTY, zwana również wartością ceny całkowitej - stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w SIWZ)

W pozycjach nr: *..... ww. tabeli obowiązek podatkowy, zgodnie z przepisami o podatku od towarów i usług, leży po stronie Zamawiającego – (***Wypełnić jeśli dotyczy**)

b) Termin dostawy:

Oferujemy dostarczenie przedmiotu zamówienia w terminie nie przekraczającym:* dni od dnia podpisania umowy.

UWAGA!!!

*NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ

(UWAGA: termin realizacji stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

c) Termin rozszerzenia wsparcia technicznego:

OKREŚLENIE ROZSZERZENIA WSPARCIA TECHNICZNEGO	<u>TAK/NIE*</u>
Wykonawca rozszerza wsparcie techniczne z 12 miesięcy na 24 miesiące.	

UWAGA!!!

*NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ

(UWAGA: wsparcie techniczne stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

Część 5 – Dostawa karty graficznej – 1 szt.
a) Cena oferty

Lp.	Zamawiany przedmiot	Oferowany przedmiot	Ilość [szt]	Cena jednostkowa netto [PLN]*	Wartość netto [PLN]*	Stawka podatku VAT (%)*	Wartość podatku VAT [PLN]*	Wartość brutto [PLN]*
A	B	C	D	E	$F = D \times E$	G	$H = F \times G$	$I = F + H$
1	Karta graficzna – 1 szt.	1) Nazwa:*..... 2) Model*..... 3) Producent *..... 4) Kraj i rok produkcji *.....	1					
2	ŁĄCZNIE		---	---		---		

(CENA OFERTY BRUTTO tj. WARTOŚĆ BRUTTO OFERTY, zwana również wartością ceny całkowitej - stanowi kryterium oceny ofert i będzie podlegała ocenie zgodnie z zasadami opisanymi w SIWZ)

W pozycjach nr: *..... ww. tabeli obowiązek podatkowy, zgodnie z przepisami o podatku od towarów i usług, leży po stronie Zamawiającego – (***Wypełnić jeśli dotyczy**)

b) Termin gwarancji:

OKREŚLENIE TERMINU GWARANCJI	<u>TAK/NIE*</u>
Wykonawca rozszerza gwarancję z 24 miesięcy na 60 miesięcy.	

UWAGA!!!

***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin gwarancji stanowi kryterium oceny ofert i będzie podlegała ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

c). Kryterium jakościowe;

	<u>TAK/NIE*</u>
Wykonawca oferują kartę graficzną z kablem wysokiej jakości wykonania DVI-HDMI 1,8m	

UWAGA!!!

***NALEŻY WPISAĆ TAK lub NIE**

(UWAGA: Kryterium jakościowe stanowi kryterium oceny ofert i będzie podlegała ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

Część 6 – Dostawa dysku wewnętrznego SSD 250 GB– 2 szt.
a) Cena oferty

Lp.	Zamawiany przedmiot	Oferowany przedmiot	Ilość [szt]	Cena jednostkowa netto [PLN]*	Wartość netto [PLN]*	Stawka podatku VAT (%)*	Wartość podatku VAT [PLN]*	Wartość brutto [PLN]*
A	B	C	D	E	$F = D \times E$	G	$H = F \times G$	$I = F + H$

1	Dostawa dysku wewnętrznego SSD 250 GB – 2 szt.	1) Nazwa:*..... 2) Model*:*..... 3) Producent *..... 4) Kraj i rok produkcji *.....	2					
2	ŁĄCZNIE		---	---		---		

(CENA OFERTY BRUTTO tj. WARTOŚĆ BRUTTO OFERTY, zwana również wartością ceny całkowitej - stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w SIWZ)

W pozycjach nr: *..... ww. tabeli obowiązek podatkowy, zgodnie z przepisami o podatku od towarów i usług, leży po stronie Zamawiającego – (***Wypełnić jeśli dotyczy**)

b) Termin gwarancji:

OKREŚLENIE GWARANCJI	TERMINU	<u>TAK/NIE*</u>
Wykonawca rozszerza gwarancję z 24 miesięcy na 60 miesięcy.		

UWAGA!!!

***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin gwarancji stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

c). Kryterium jakościowe;

	<u>TAK/NIE*</u>
Wykonawca oferuję do każdego dysku ramki umożliwiające zamontowanie dysku twardego SSD o wielkości 2,5 cala do zatoki 3,5 cala w komputerach PC	

UWAGA!!!

***NALEŻY WPISAĆ TAK lub NIE**

(UWAGA: Kryterium jakościowe stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

Część 7 – Dostawa pamięci RAM 4 GB – 1 szt.

a) Cena oferty

Lp.	Zamawiany przedmiot	Oferowany przedmiot	Ilość [szt]	Cena jednostkowa netto [PLN]*	Wartość netto [PLN]*	Stawka podatku VAT (%)*	Wartość podatku VAT [PLN]*	Wartość brutto [PLN]*
A	B	C	D	E	F= D x E	G	H = F x G	I = F + H
1	Pamięć RAM 4 GB – szt.	1) Nazwa:*..... 2) Model*:*..... 3) Producent *..... 4) Kraj i rok produkcji *.....	1					
2	ŁĄCZNIE		---	---		---		

(CENA OFERTY BRUTTO tj. WARTOŚĆ BRUTTO OFERTY, zwana również wartością ceny całkowitej - stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w SIWZ)

W pozycjach nr: *..... ww. tabeli obowiązek podatkowy, zgodnie z przepisami o podatku od towarów i usług, leży po stronie Zamawiającego – (***Wypełnić jeśli dotyczy**)

b) Termin dostawy:

Oferujemy dostarczenie przedmiotu zamówienia w terminie nie przekraczającym:* dni od dnia podpisania umowy.

UWAGA!!!

***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin realizacji stanowi kryterium oceny ofert i będzie podlegał ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

c) Termin gwarancji:

OKREŚLENIE GWARANCJI	TERMINU	TAK/NIE*
Wykonawca rozszerza gwarancję z 24 miesięcy na 60 miesięcy.		

UWAGA!!!

***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin gwarancji stanowi kryterium oceny ofert i będzie podlegał ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

Część 8 – Dostawa karty micro SD 256 GB – 10 szt.

a) Cena oferty

Lp.	Zamawiany przedmiot	Oferowany przedmiot	Ilość [szt]	Cena jednostkowa netto [PLN]*	Wartość netto [PLN]*	Stawka podatku VAT (%)*	Wartość podatku VAT [PLN]*	Wartość brutto [PLN]*
A	B	C	D	E	$F = D \times E$	G	$H = F \times G$	$I = F + H$
1	Karta micro SD 256 GB – 10 szt.	1) Nazwa:*..... 2) Model*:*..... 3) Producent *..... 4) Kraj i rok produkcji *.....	10					
2	ŁĄCZNIE		---	---		---		

(CENA OFERTY BRUTTO tj. WARTOŚĆ BRUTTO OFERTY, zwana również wartością ceny całkowitej - stanowi kryterium oceny ofert i będzie podlegał ocenie zgodnie z zasadami opisanymi w SIWZ)

W pozycjach nr: *..... ww. tabeli obowiązek podatkowy, zgodnie z przepisami o podatku od towarów i usług, leży po stronie Zamawiającego – (***Wypełnić jeśli dotyczy**)

b) Termin gwarancji:

OKREŚLENIE TERMINU GWARANCJI	<u>TAK/NIE*</u>
Wykonawca rozszerza gwarancję z 36 miesięcy na 60 miesięcy.	

UWAGA!!!
***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin gwarancji stanowi kryterium oceny ofert i będzie podlegał ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

c) Kryterium jakościowe;

	<u>TAK/NIE*</u>
Wykonawca oferuje dostarczenie adaptera z microSD na kartę SD	

UWAGA!!!
***NALEŻY WPISAĆ TAK lub NIE**

(UWAGA: Kryterium jakościowe stanowi kryterium oceny ofert i będzie podlegał ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

Część 9 – Dostawa dysku wewnętrznego 500 GB –1 szt.,
a) Cena oferty

Lp.	Zamawiany przedmiot	Oferowany przedmiot	Ilość [szt]	Cena jednostkowa netto [PLN]*	Wartość netto [PLN]*	Stawka podatku VAT (%)*	Wartość podatku VAT [PLN]*	Wartość brutto [PLN]*
A	B	C	D	E	$F = D \times E$	G	$H = F \times G$	$I = F + H$
1	Dysk wewnętrzny 500 GB – 1 szt.	1) Nazwa:*..... 2) Model:*..... 3) Producent *..... 4) Kraj i rok produkcji *.....	1					
2		ŁĄCZNIE	---	---		---		

(CENA OFERTY BRUTTO tj. WARTOŚĆ BRUTTO OFERTY, zwana również wartością ceny całkowitej - stanowi kryterium oceny ofert i będzie podlegał ocenie zgodnie z zasadami opisanymi w SIWZ)

W pozycjach nr: *..... ww. tabeli obowiązek podatkowy, zgodnie z przepisami o podatku od towarów i usług, leży po stronie Zamawiającego – (*Wypełnić jeśli dotyczy)

b) Termin dostawy:

Oferujemy dostarczenie przedmiotu zamówienia w terminie nie przekraczającym:* dni od dnia podpisania umowy.

UWAGA!!!
***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin realizacji stanowi kryterium oceny ofert i będzie podlegał ocenie zgodnie z zasadami opisanymi)



w rozdziale XIII SIWZ)

c) Termin gwarancji:

OKREŚLENIE GWARANCJI	TERMINU	TAK/NIE*
Wykonawca rozszerza gwarancję z 36 miesięcy na 60 miesięcy.		

UWAGA!!!

***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin gwarancji stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

Część 10 – Dostawa pakietu bezpieczeństwa antywirusowego przeznaczonego do ochrony komputerów – licencja – 250 szt., pakietu ochrony skrzynek pocztowych – licencja – 200 szt., pakietu ochrony urządzeń mobilnych – licencja – 5 szt.

a) Cena oferty

Lp.	Zamawiany przedmiot	Oferowany przedmiot	Ilość [szt]	Cena jednostkowa netto [PLN]*	Wartość netto [PLN]*	Stawka podatku VAT (%)*	Wartość podatku VAT [PLN]*	Wartość brutto [PLN]*
A	B	C	D	E	$F = D \times E$	G	$H = F \times G$	$I = F + H$
1	pakietu bezpieczeństwa antywirusowego przeznaczonego do ochrony komputerów – licencja – 250 szt.	1) Nazwa:*..... 2) Producent *..... 3) Typ oprogramowania*.....	250					
2	pakietu ochrony skrzynek pocztowych – licencja – 200 szt	1) Nazwa:*..... 2) Producent *..... 3) Typ oprogramowania*.....	200					
3	pakietu ochrony urządzeń mobilnych – licencja – 5 szt	1) Nazwa:*..... 2) Producent *..... 3) Typ oprogramowania*.....	5					
4	ŁĄCZNIE		---	---		---		

(CENA OFERTY BRUTTO tj. WARTOŚĆ BRUTTO OFERTY, zwana również wartością ceny całkowitej - stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w SIWZ)

W pozycjach nr: *..... ww. tabeli obowiązek podatkowy, zgodnie z przepisami o podatku od towarów i usług, leży po stronie Zamawiającego – (***Wypełnić jeśli dotyczy**)

b) Termin dostawy:

Oferujemy dostarczenie przedmiotu zamówienia w terminie nie przekraczającym:
* dni od dnia podpisania umowy.

UWAGA!!!

***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin realizacji stanowi kryterium oceny ofert i będzie podlegał ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

c) Kryterium jakościowe:

	<u>TAK/NIE*</u>
Wykonawca zaoferuje dodatkowo dwie licencje na oprogramowanie do ochrony urządzeń mobilnych.	

UWAGA!!!

***NALEŻY WPISAĆ TAK lub NIE**

(UWAGA: Kryterium jakościowe stanowi kryterium oceny ofert i będzie podlegał ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

Część 11 – Dostawa komputerów stacjonarnych – 4 szt.
a) Cena oferty

Lp.	Zamawiany przedmiot	Oferowany przedmiot	Ilość [szt]	Cena jednostkowa netto [PLN]*	Wartość netto [PLN]*	Stawka podatku VAT (%)*	Wartość podatku VAT [PLN]*	Wartość brutto [PLN]*
A	B	C	D	E	$F = D \times E$	G	$H = F \times G$	$I = F + H$
1	Komputer stacjonarny – 4 szt.	1) Nazwa:*..... 2) Model*..... 3) Producent *..... 4) Kraj i rok produkcji *.....	4					
2		ŁĄCZNIE	---	---		---		

(CENA OFERTY BRUTTO tj. WARTOŚĆ BRUTTO OFERTY, zwana również wartością ceny całkowitej - stanowi kryterium oceny ofert i będzie podlegał ocenie zgodnie z zasadami opisanymi w SIWZ)

W pozycjach nr: *..... ww. tabeli obowiązek podatkowy, zgodnie z przepisami o podatku od towarów i usług, leży po stronie Zamawiającego – (***Wypełnić jeśli dotyczy**)

b). Termin gwarancji:

OKREŚLENIE TERMINU GWARANCJI	<u>TAK/NIE*</u>
Wykonawca rozszerza gwarancję z 24 miesięcy na 36 miesięcy.	

UWAGA!!!

***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin gwarancji stanowi kryterium oceny ofert i będzie podlegał ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

w rozdziale XIII SIWZ)

c). Kryterium jakościowe;

	<u>TAK/NIE*</u>
Wykonawca oferują dodatkowo klawiaturę i mysz bezprzewodową	

UWAGA!!!

***NALEŻY WPISAĆ TAK lub NIE**

(UWAGA: Kryterium jakościowe stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

Część 12 – Dostawa monitorów 24 cale – 5 szt.

a) Cena oferty

Lp.	Zamawiany przedmiot	Oferowany przedmiot	Ilość [szt]	Cena jednostkowa netto [PLN]*	Wartość netto [PLN]*	Stawka podatku VAT (%)*	Wartość podatku VAT [PLN]*	Wartość brutto [PLN]*
A	B	C	D	E	$F = D \times E$	G	$H = F \times G$	$I = F + H$
1	Monitor 24 cale – 5 szt.	1) Nazwa: *..... 2) Model: *..... 3) Producent *..... 4) Kraj i rok produkcji *.....	5					
2		ŁĄCZNIE	---	---		---		

(CENA OFERTY BRUTTO tj. WARTOŚĆ BRUTTO OFERTY, zwana również wartością ceny całkowitej - stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w SIWZ)

W pozycjach nr: *..... ww. tabeli obowiązków podatkowy, zgodnie z przepisami o podatku od towarów i usług, leży po stronie Zamawiającego – (***Wypełnić jeśli dotyczy**)

b). Termin gwarancji:

OKREŚLENIE TERMINU GWARANCJI	<u>TAK/NIE*</u>
Wykonawca rozszerza gwarancję z 36 miesięcy na 60 miesięcy.	

UWAGA!!!

***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin gwarancji stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

c). Kryterium jakościowe;

	<u>TAK/NIE*</u>
Wykonawca oferując kabel wysokiej jakości DVI męska-HDMI 1,8 m, pozłacane końcówki złącz	

UWAGA!!!
***NALEŻY WPISAĆ TAK lub NIE**

(UWAGA: Kryterium jakościowe stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

Część 13 – Dostawa listwy głośnikowej dedykowanej do monitora – 5 szt.
a) Cena oferty

Lp.	Zamawiany przedmiot	Oferowany przedmiot	Ilość [szt]	Cena jednostkowa netto [PLN]*	Wartość netto [PLN]*	Stawka podatku VAT (%)*	Wartość podatku VAT [PLN]*	Wartość brutto [PLN]*
A	B	C	D	E	$F = D \times E$	G	$H = F \times G$	$I = F + H$
1	Listwa głośnikowa dedykowana do monitora – 5 szt.	1) Nazwa:*..... 2) Model*:*..... 3) Producent *..... 4) Kraj i rok produkcji *.....	5					
2		ŁĄCZNIE	---	---		---		

(CENA OFERTY BRUTTO tj. WARTOŚĆ BRUTTO OFERTY, zwana również wartością ceny całkowitej - stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w SIWZ)

 W pozycjach nr: *..... ww. tabeli obowiązek podatkowy, zgodnie z przepisami o podatku od towarów i usług, leży po stronie Zamawiającego – (***Wypełnić jeśli dotyczy**)

b) Termin dostawy:
Oferujemy dostarczenie przedmiotu zamówienia w terminie nie przekraczającym:
* dni od dnia podpisania umowy.

UWAGA!!!
***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin realizacji stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

c) Termin gwarancji:

OKREŚLENIE TERMINU GWARANCJI	<u>TAK/NIE*</u>
Wykonawca rozszerza gwarancję z 12 miesięcy na 24 miesiące.	

UWAGA!!!
***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin gwarancji stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

Część 14 – Dostawa zestawów „klawiatura i mysz bezprzewodowa” – 7 szt.

a) Cena oferty

Lp.	Zamawiany przedmiot	Oferowany przedmiot	Ilość [szt]	Cena jednostkowa netto [PLN]*	Wartość netto [PLN]*	Stawka podatku VAT (%)*	Wartość podatku VAT [PLN]*	Wartość brutto [PLN]*
A	B	C	D	E	$F = D \times E$	G	$H = F \times G$	$I = F + H$
1	zestaw „klawiatura i mysz bezprzewodowa” – 7 szt.	1) Nazwa:*..... 2) Model*:*..... 3) Producent *..... 4) Kraj i rok produkcji *.....	7					
2		ŁĄCZNIE	---	---		---		

(CENA OFERTY BRUTTO tj. WARTOŚĆ BRUTTO OFERTY, zwana również wartością ceny całkowitej - stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w SIWZ)

W pozycjach nr: *..... ww. tabeli obowiązek podatkowy, zgodnie z przepisami o podatku od towarów i usług, leży po stronie Zamawiającego – (***Wypełnić jeśli dotyczy**)

b) Termin dostawy:

Oferujemy dostarczenie przedmiotu zamówienia w terminie nie przekraczającym:* dni od dnia podpisania umowy.

UWAGA!!!

***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin realizacji stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

c) Termin gwarancji:

OKREŚLENIE TERMINU GWARANCJI	<u>TAK/NIE*</u>
Wykonawca rozszerza gwarancję z 24 miesięcy na 36 miesięcy.	

UWAGA!!!

***NALEŻY WPISAĆ TERMIN OFEROWANY PRZEZ WYKONAWCĘ**

(UWAGA: termin gwarancji stanowi kryterium oceny ofert i będzie podlegać ocenie zgodnie z zasadami opisanymi w rozdziale XIII SIWZ)

- Oświadczamy, że zapoznaliśmy się z treścią SIWZ i nie wnosimy do niej żadnych uwag i zastrzeżeń.
- Zobowiązujemy się do wykonania zamówienia w terminie określonym w SIWZ.



4. Oświadczamy, że uważamy się za związanych niniejszą ofertą przez okres **30 dni** licząc od upływu ostatecznego terminu składania ofert.
5. Udzielamy gwarancji i rękojmi na dostawy objęte przedmiotem zamówienia na okres wskazany w siwz.
6. Wyrażamy zgodę na warunki płatności określone przez Zamawiającego w SIWZ.
7. Oświadczamy, że wzór umowy wraz z załącznikami został przez nas zaakceptowany bez zastrzeżeń; w przypadku wyboru naszej oferty, zobowiązujemy się do zawarcia umowy na warunkach określonych we wzorach oraz w miejscu i terminie wyznaczonym przez Zamawiającego.
8. W przypadku uznania naszej oferty za najkorzystniejszą zobowiązujemy się zawrzeć umowę konsorcjum lub inną równoważną umowę, zgodnie z treścią SIWZ (dotyczy Wykonawców wspólnie składających ofertę).
9. Oświadczam, że wypełniłam/em obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO (rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1)) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu (w przypadku, gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca).
10. Oferta została złożona na stronach.
11. Załącznikami do niniejszej oferty są:
 - a)
 - b)
 - c)

12. Wszelką korespondencję w sprawie niniejszego zamówienia należy kierować na adres

..... tel./fax.

....., dnia:2019 r.

.....
(Podpis osoby upoważnionej do reprezentowania wykonawcy)

Oświadczenie wykonawcy

Instrukcja wypełniania:

1. Dokument „Oświadczenie Wykonawcy” obejmuje oficjalne oświadczenie Wykonawcy stwierdzające, że spełnia warunki udziału w postępowaniu i nie podlega wykluczeniu z udziału w postępowaniu. *
2. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenie niniejsze składa każdy Wykonawca.*
3. 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 zamieszcza informacje o tych podmiotach w oświadczeniu.*
4. Wykonawca, który zamierza powierzyć część zamówienia podwykonawcy zamieszcza informacje o tych podwykonawcach w oświadczeniu. *
5. Wykonawca powinien wyraźnie zaznaczyć jeden z wariantów wyboru (np. „tak/nie/nie dotyczy/pełnomocnikiem/Liderem) najlepiej poprzez wykreślenie odpowiedzi niewłaściwej.*

* **niepotrzebne skreślić**

Nazwa zamówienia: Dostawa laptopów z oprogramowaniem, licencji oraz akcesoriów komputerowych dla Instytutu Agrofizyki im. B. Dobrzańskiego Polskiej Akademii Nauk w Lublinie z podziałem na 14 części A-2401-9/2019		
Lp.	Informacje wymagane przez Zamawiającego	Wypełnia Wykonawca
SEKCJA I: INFORMACJE DOTYCZĄCE WYKONAWCY		
A	Informacje na temat Wykonawcy	
1.	Nazwa Wykonawcy/ Imię i nazwisko	
2.	Adres pocztowy	
3.	Telefon	
4.	Adres e:mail	
5.	Faks	
6.	NIP	
7.	REGON	
8.	Czy Wykonawca jest małym lub średnim przedsiębiorcą?	*TAK / *NIE
B	Informacje na temat wspólnego ubiegania się o udzielenie zamówienia publicznego	
9.	Czy Wykonawca bierze udział w niniejszym postępowaniu o udzielenie zamówienia publicznego wspólnie i innymi Wykonawcami?	*TAK / *NIE
10.	Jeżeli w ww. punktach odpowiedź jest twierdząca, należy wskazać pozostałych Wykonawców biorących udział w postępowaniu o udzielenie zamówienia publicznego	
11.	W przypadku Wykonawców występujących wspólnie – w rozumieniu art. 23 ust. 2 ustawy Pzp, należy wskazać pełnomocnika lub lidera (wypełnić jeżeli dotyczy)	*Pełnomocnikiem / * Liderem
C	Informacje na temat przedstawicieli prawnych Wykonawcy	
12.	Pełnomocnik(-cy), osoby uprawnione: Należy podać osobę(-y) – imię(-iona) i nazwisko(-a)	



	osoby (osób) upoważnionej (-ych) do prawnego reprezentowania Wykonawcy (-ów) na potrzeby niniejszego postępowania	
13.	Osoba wyznaczona do kontaktów ze strony Wykonawcy, w tym do otrzymywania i wymiany korespondencji w ramach niniejszego postępowania: Imię i nazwisko, stanowisko, dane kontaktowe, teleadresowe	
D	Informacje na temat polegania na zdolności innych podmiotów	
14	Czy Wykonawca polega na zdolności innych podmiotów w celu spełnienia warunków udziału w postępowaniu określonych poniżej w sekcji II	*TAK / *NIE
15	Jeżeli w ww. pkt. odpowiedź jest twierdząca, Wykonawca winien przedstawić: a. dane tych podmiotów b. informacje wymagane w sekcji II oraz sekcji IV oświadczenia - dla każdego z podmiotów, których to dotyczy (<i>sekcję II i sekcję IV należy wypełnić w odniesieniu do każdego podmiotu osobno</i>)	
Sekcja II: WARUNKI UDZIAŁU W POSTĘPOWANIU:		
<p>Wypełnić, gdy Wykonawca spełnia warunki samodzielnie. Jeżeli Wykonawca samodzielnie spełnia jedynie jeden z niżej wymienionych warunków, należy wykreślić warunek którego Wykonawca nie spełnia.</p> <p>W przypadku polegania na zasobach podmiotu trzeciego w trybie art. 22a ustawy Pzp, sekcję II należy wypełnić osobno w odniesieniu do tego podmiotu wypełniając wiersze dotyczące warunku wykazywanego przez ten podmiot a wykreślając pozostałe warunki</p> <p>W przypadku polegania na zasobach podmiotu trzeciego w trybie art. 22a ustawy, do oświadczenia dotyczącego podmiotu, Wykonawca winien dołączyć dowody, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tego podmiotu (tych podmiotów), w szczególności przedstawiając zobowiązanie tego podmiotu (tych podmiotów) do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia</p>		
	<p>Oświadczam, że Wykonawca:</p> <p>(Wpisać Wykonawcę, jeśli wykonawca samodzielnie spełnia warunek. Jeśli warunek będzie wykazywany przez podmiot trzeci w trybie art. 22a Pzp, sekcję II należy wypełnić osobno w odniesieniu do tego podmiotu podając tu podmiot, którym Wykonawca wykazuje spełnienie warunku)</p>	
SEKCJA III: PODSTAWY WYKLUCZENIA		
<p>W przypadku polegania na zasobach podmiotu trzeciego w trybie art. 22 a ustawy Pzp do oświadczenia Wykonawca powinien dołączyć dowody, 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</p>		
	Oświadczam, że Wykonawca:	
16.	Czy Wykonawca podlega wykluczeniu na podstawie któregośkolwiek z przepisów wskazanych: • w art. 24 ust. 1 pkt 12-23 ustawy Pzp	*TAK / *NIE
17.	Jeżeli w ww. pkt. odpowiedź jest twierdząca, należy wskazać na podstawie której przesłanki Wykonawca podlega wykluczeniu oraz uzasadnić (podać przyczyny faktyczne)	
18.	Czy Wykonawca w przypadku występowania przesłanek wykluczenia wskazanych w art. 24 ust. 1 pkt 13 i 14 oraz 16-20 ustawy Pzp podejmuje próbę wykazania rzetelności określoną w art. 24 ust. 8	*TAK / *NIE / *NIE DOTYCZY



	ustawy Pzp?	
19.	Jeżeli w ww. pkt odpowiedź jest twierdząca, należy wskazać dowody wykazujące rzetelność Wykonawcy (art. 24 ust. 8 Pzp)	
SEKCJA IV: PODWYKONAWSTWO		
Sekcję wypełnia Wykonawca tylko wtedy, gdy zamierza powierzyć wykonanie części zamówienia podwykonawcy (-om)		
20.	Realizację zamówienia zamierzamy powierzyć podwykonawcy (-om) w części wg zakresu robót/prac: (Wypełnić jeżeli dotyczy – należy podać proponowanego podwykonawcę/ów oraz wskazać zakres robót przewidzianych do wykonania przez tego podwykonawcę/-ów)	1) - 2) -
21.	Czy podwykonawca wskazany w ww. punkcie podlega wykluczeniu na podstawie któregośkolwiek z przepisów wskazanych w art.: - w art. 24 ust. 1 pkt. 13-22 ustawy Pzp (W przypadku pozytywnej odpowiedzi, należy wskazać, których podwykonawców dotyczy wykluczenie, jeśli wykonawca przewiduje więcej niż jednego podwykonawcę.)	*TAK / *NIE w odniesieniu do podwykonawcy(-ów):
22.	Jeżeli w ww. pkt. odpowiedź jest twierdząca, należy wskazać na podstawie której przesłanki podwykonawca podlega wykluczeniu oraz uzasadnić (podać przyczyny faktyczne)	
23.	Czy podwykonawca, w przypadku występowania przesłanek wykluczenia wskazanych w art. 24 ust. 1 pkt. 13 i 14 oraz 16-20 ustawy Pzp podejmuje próbę wykazania rzetelności określoną w art. 24 ust. 8 ustawy Pzp?: (W przypadku pozytywnej odpowiedzi, należy wskazać, których podwykonawców dotyczy)	*TAK / *NIE / *NIE DOTYCZY
24.	Jeżeli w ww. pkt. odpowiedź jest twierdząca, należy wskazać dowody wykazujące rzetelność (art. 24 ust. 8 Pzp) wykonawcy	
Sekcja V: WSKAZANIE PRZEZ WYKONAWCĘ DOSTĘPNOŚCI OŚWIADCZEŃ I DOKUMENTÓW (wypełnić o ile dotyczy)		
<i>Zamawiający może zażądać od Wykonawcy przedstawienia tłumaczenia na język polski wskazanych przez Wykonawcę i pobranych samodzielnie przez Zamawiającego oświadczeń i dokumentów</i>		
25.	Jeśli oświadczenie lub dokument potwierdzający brak podstaw wykluczenia na podstawie art. 24 ust. 5 pkt 1 ustawy Pzp dostępny jest w formie elektronicznej proszę wskazać:	adres internetowy pod którym Zamawiający może uzyskać bezpłatny dostęp do dokumentu: KRS* -....., CEIDG* -..... inne (...)*-.....
26.	Jeśli oświadczenie lub dokument potwierdzający spełnienie warunków udziału w postępowaniu lub braku podstaw wykluczenia (o ile będą one aktualne) znajdują się w posiadaniu Zamawiającego proszę wskazać:	Numer sprawy / postępowania do którego Wykonawca złożył wskazane oświadczenia i dokumenty: 1. Nr sprawy Wymienić oświadczenie/dokument 2. Nr sprawy Wymienić oświadczenie/dokument 3. Nr sprawy Wymienić oświadczenie/dokument
SEKCJA VI: OŚWIADCZENIA KOŃCOWE		
27.	Ja, niżej podpisany, oświadczam, że informacje podane przeze mnie są dokładne i prawdziwe oraz, że jestem świadomy konsekwencji podania nieprawdziwych informacji. Zgodnie z art. 297 § 1 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. z 1997 r. Nr 88, poz. 553 z	



późn.zm.): „Kto, w celu uzyskania od organu lub instytucji dysponujących środkami publicznymi zamówienia publicznego, przedkłada poświadczający nieprawdę albo nierzetelny dokument albo nierzetelne, pisemne oświadczenie dotyczące okoliczności o istotnym znaczeniu dla uzyskania zamówienia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5”.

..... (miejsowość), dnia r.

.....
(czytelny podpis lub podpis i pieczętka imienna
upoważnionych przedstawicieli Wykonawcy)

Oświadczenie wykonawcy

Instrukcja wypełniania:

Dokument „Oświadczenie Wykonawcy” obejmuje oficjalne oświadczenie Wykonawcy stwierdzające, że spełnia warunki udziału w postępowaniu

*** niepotrzebne skreślić**

<p>Nazwa zamówienia: Dostawa laptopów z oprogramowaniem, licencji oraz akcesoriów komputerowych dla Instytutu Agrofizyki im. B. Dobrzańskiego Polskiej Akademii Nauk w Lublinie z podziałem na 14 części</p> <p>A-2401-9/2019</p>		
Lp.	Informacje wymagane przez Zamawiającego	Wypełnia Wykonawca
SEKCJA I: SPEŁNIENIE WARUNKÓW		
Oświadczam, że Wykonawca:		
1.	Wykonawca spełnia warunki udziału w postępowaniu określone przez Zamawiającego w pkt V specyfikacji istotnych warunków zamówienia.	*TAK / *NIE
SEKCJA IV: OŚWIADCZENIA KOŃCOWE		
2.	Ja, niżej podpisany, oświadczam, że informacje podane przeze mnie są dokładne i prawidłowe oraz, że jestem świadomy konsekwencji podania nieprawdziwych informacji. Zgodnie z art. 297 § 1 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. z 1997 r. Nr 88, poz. 553 z późn.zm.): „Kto, w celu uzyskania od organu lub instytucji dysponujących środkami publicznymi zamówienia publicznego, przedkłada poświadczający nieprawdę albo nierzetelny dokument albo nierzetelne, pisemne oświadczenie dotyczące okoliczności o istotnym znaczeniu dla uzyskania zamówienia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5”.	

..... (miejscowość), dnia r.

.....
 (czytelny podpis lub podpis i pieczęć imienna
 upoważnionych przedstawicieli Wykonawcy)

Załącznik nr 4 do SIWZ

**NALEŻY PRZEKAZAĆ ZAMAWIAJACEMU W CIĄGU 3 DNI OD DNIA PRZEKAZANIA
INFORMACJI, O KTÓRYCH MOWA W ART. 86 UST. 5 USTAWY PZP**

WYKONAWCA:

Lp.	Nazwa(y) Wykonawcy(ów)	NIP	REGON	Adres(y) Wykonawcy(ów)	Numer tel i faksu, adres e:mailowy
1.					

Oświadczenie wykonawcy

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

Prawo zamówień publicznych (dalej jako: ustawa PZP),

DOTYCZĄCE PRZYNALEŻNOŚCI LUB BRAKU PRZYNALEŻNOŚCI

DO GRUPY KAPITAŁOWEJ

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Dostawa laptopów z oprogramowaniem, licencji oraz akcesoriów komputerowych dla Instytutu Agrofizyki im. B. Dobrzańskiego Polskiej Akademii Nauk w Lublinie z podziałem na 14 części A-2401-9/2019.**

oświadczam, co następuje:

INFORMACJA DOTYCZĄCA WYKONAWCY:

przedkładam informację, w trybie art. 24 ust. 11 ustawy PZP o tym, że na dzień składania ofert:

nie należę do grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy PZP; *

należę do grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy PZP. *

..... (miejsowość), dnia r.

.....
(podpis)

*Skreślić niewłaściwe

UWAGA!

a) Wykonawca przekazuje dokument Zamawiającemu bez wzywania

b) W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, niniejsze oświadczenie powinien złożyć każdy z tych Wykonawców

Załącznik nr 5.1 do SIWZ

Część 1; 11

UMOWA NR

W dniu2019 r. w Lublinie pomiędzy,
zwanym w treści umowy ZAMAWIAJĄCYM, reprezentowanym przez

1.

a działającą (-ym) na podstawie wpisu do pod numerem,
zwaną (-ym) w dalszej części umowy WYKONAWCĄ, reprezentowaną (-ym) przez:

1.

w wyniku postępowania o udzielenie zamówienia publicznego przeprowadzonego w trybie przetargu nieograniczonego na: dostawę laptopów z oprogramowaniem, licencji oraz akcesoriów komputerowych dla Instytutu Agrofizyki im. B. Dobrzańskiego Polskiej Akademii Nauk w Lublinie z podziałem na 14 części A-2401-9/2019

W części 1 i 8 Zamówienie finansowane z środków otrzymanych od Narodowego Centrum Badań i Rozwoju na realizację projektu: „Sonda profilowa TDT do pomiaru wilgotności, temperatury i elektrycznej przewodności gleby” (akronim: PROFILE-TDT) nr umowy STAIR/5/2016

W części 2; 3; 4; 6; 7; 10; 11; 12; 13; 14 Środki własne Instytutu Agrofizyki im. B. Dobrzańskiego Polskiej Akademii Nauk
W części 1; 5; 8 i 9 Zamówienie finansowane z środków otrzymanych od Narodowego Centrum Badań i Rozwoju na realizację projektu „Mobilny system iniekcyjnego, precyzyjnego nawadniania i nawożenia, zaspokajający indywidualne potrzeby rośliny” (Akronim: MSINiN), nr umowy: BIOSTRATEG3/343547/8/NCBR/2017)

została zawarta umowa o następującej treści:

§ 1

1. Wykonawca zobowiązuje się sprzedać, dostarczyć do siedziby Zamawiającego spełniający warunki określone w Specyfikacji Istotnych Warunków Zamówienia (SIWZ), stanowiącej załącznik nr 1 do niniejszej umowy oraz w złożonej ofercie i załączonym do niej zestawieniu wymaganych parametrów technicznych i użytkowych (oferta wraz z zestawieniem – załącznik nr 2 do umowy), zwane dalej przedmiotem umowy.

2. Wykonawca dostarczy przedmiot umowy wraz z dokumentami licencji* udzielonej na czas nieoznaczony na oprogramowanie wskazane w opisie przedmiotu umowy zawartym w SIWZ (załącznik nr 1 do umowy). Wykonawca oświadcza, że dysponuje prawem udzielenia licencji do tego oprogramowania.

*o ile dotyczy

3. Koszty dostawy wraz z kosztami opakowania i ubezpieczenia ponosi Wykonawca.

4. Przedmiot umowy będzie dostarczony w opakowaniu zabezpieczonym przed uszkodzeniem w czasie transportu.
5. Wykonawca gwarantuje, iż przedmiot umowy jest fabrycznie nowy, ma należyłą jakość, funkcjonalność i parametry techniczne.

§ 2

1. Wykonanie umowy, tj. dostawa przedmiotu umowy nastąpi w terminie:

- a) Dla części 1 maksymalnie do dni kalendarzowych licząc od dnia podpisania umowy.*
- b) Dla części 11 maksymalnie do 14 dni kalendarzowych licząc od dnia podpisania umowy.*

* odpowiednie zostawić

2. Wykonawca jest zobowiązany zawiadomić Zamawiającego o gotowości dostawy przedmiotu umowy nie później niż na 1 dzień roboczy przed dostawą.
3. Po dostawie i przetestowaniu przedmiotu umowy Zamawiający dokona jego odbioru, który nastąpi poprzez podpisanie przez strony protokołu odbioru bez zastrzeżeń. Podpisanie protokołu odbioru z zastrzeżeniami wywołuje skutki równoznaczne ze zwłoką w wykonaniu umowy, jeżeli upłynął termin, o którym mowa w ust. 1.

§ 3

1. Na przedmiot umowy Wykonawca udziela gwarancji na okres wskazany w ofercie Wykonawcy wraz z zestawieniem wymaganych parametrów technicznych i użytkowych (załącznik nr 2 do umowy).
2. Gwarancja liczona jest od dnia podpisania bez zastrzeżeń protokołu odbioru przedmiotu umowy.
3. Gwarancja obejmuje wszystkie wykryte podczas eksploatacji przedmiotu umowy usterki i wady oraz uszkodzenia powstałe w czasie poprawnego, zgodnego z instrukcją jego użytkowania.
4. Serwis gwarancyjny świadczony będzie w miejscu użytkowania przedmiotu umowy. W przypadku niemożności dokonania naprawy na miejscu i konieczności dostarczenia przedmiotu umowy do punktu serwisowego wskazanego przez Wykonawcę – koszty dostarczenia do punktu serwisowego oraz z punktu serwisowego do miejsca siedziby Zamawiającego pokrywa Wykonawca.
5. Wykonawca przystąpi do usunięcia awarii – niezwłocznie po otrzymaniu informacji o awarii.
6. Wady ujawnione w okresie gwarancyjnym będą usunięte w terminie 14 dni od dnia ich zgłoszenia.
7. Jeżeli opóźnienie w naprawie przedmiotu umowy w stosunku do terminu określonego w ust. 6 przekroczy 14 dni Wykonawca zobowiązuje się do wymiany przedmiotu umowy na nowy, wolny od wad. Do momentu wymiany przedmiotu umowy Wykonawca pozostaje w opóźnieniu w usunięciu wad, chyba że wymiana nastąpiła w terminie określonym w ust. 6 w ramach usunięcia zgłoszonej wady.
8. Okres gwarancji ulega przedłużeniu o czas naprawy przedmiotu umowy, przy czym Zamawiający może dochodzić roszczeń z tytułu gwarancji także po jej upływie, jeżeli zgłoszenie wady miało miejsce przed jej upływem.

9. Zgłoszenia uszkodzeń będą przyjmowane drogą elektroniczną (e-mail), telefoniczną i faksową na nr we wszystkie dni robocze w godzinach 8.00 – 15.00.
10. W okresie gwarancji Zamawiający ma prawo do:
 - dysponowania przedmiotem umowy.
11. Niezależnie od uprawnień z tytułu gwarancji, Zamawiający może wykonywać uprawnienia z tytułu rękojmi na zasadach ogólnych z tym, że okres rękojmi jest równy okresowi gwarancji.
12. Wykonawca zapewni na przedmiot umowy odpłatny serwis pogwarancyjny przez okres co najmniej 24 miesięcy od daty upływu terminu gwarancji, stosując średnie ceny z rynku polskiego.

§ 4

1. Za wykonanie umowy Wykonawca otrzyma wynagrodzenie w wysokości:
 - netto: (słownie:)
 - VAT: (słownie:)
 - Brutto: (słownie:)**
2. Wynagrodzenie, o którym mowa w ust. 1 obejmuje wszelkie koszty związane z realizacją przedmiotu umowy w tym w szczególności koszt opakowania, dostarczenia, ubezpieczenia na czas transportu, świadczenia usług serwisu gwarancyjnego, koszt udzielenia licencji do oprogramowania oraz wszelkie należne opłaty i podatki, w tym podatek VAT.
3. Wykonawca wystawi Zamawiającemu fakturę za przedmiot umowy po podpisaniu przez Strony bez zastrzeżeń protokołu odbioru.
4. Faktura, której załącznikiem będzie protokół odbioru, wystawiona będzie na, NIP:
5. Po przedstawieniu przez Wykonawcę faktury wraz z załącznikiem, zgodnie z ust. 4, Zamawiający zapłaci należność wynikającą z tej faktury przelewem na konto Wykonawcy – w terminie 30 dni, licząc od daty jej doręczenia Zamawiającemu.
6. Przyjmuje się, że dniem zapłaty jest dzień obciążenia rachunku bankowego Zamawiającego.

§ 5

1. Wykonawca zapłaci Zamawiającemu kary umowne:
 - a) za zwłokę w wykonaniu umowy, tj. dostawie, zainstalowaniu, uruchomieniu przedmiotu umowy, w wysokości 0,4% wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy, za każdy dzień zwłoki, przy czym łączna kara umowna z tego tytułu nie może przekroczyć 10 % wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy;
 - b) za opóźnienie w usunięciu wad w stosunku do terminu określonego w § 3 ust. 6 umowy, w wysokości 0,4% wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy, za każdy dzień opóźnienia, przy czym łączna kara umowna z tego tytułu nie może przekroczyć 10 % wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy;



c) za odstąpienie od umowy przez Zamawiającego z przyczyn, za które ponosi odpowiedzialność Wykonawca, jak również za odstąpienie od umowy przez Wykonawcę z przyczyn leżących po jego stronie w wysokości 10% wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy.

2. Wykonawca wyraża zgodę na potrącenie kar umownych z przysługującego mu wynagrodzenia.

3. Zamawiający ma prawo dochodzić odszkodowania uzupełniającego na zasadach Kodeksu Cywilnego, jeżeli szkoda przewyższy wysokość kar umownych.

4. Wykonawcy od faktur niezapłaconych w terminie określonym w § 4 ust. 5 przysługują odsetki ustawowe.

5. Zamawiający ma prawo odstąpić od umowy ze skutkiem natychmiastowym z przyczyn, za które odpowiedzialność ponosi Wykonawca, w szczególności jeżeli:

a) zwłoka w wykonaniu umowy wynosi 14 dni, przy czym dostarczenie przedmiotu umowy w stanie niekompletnym, z wadą, niespełniającego wymagań określonych przez Zamawiającego wywołuje skutki równoznaczne ze zwłoką w jej wykonaniu, jeżeli upłynął termin, o którym mowa w § 2 ust. 1.

b) Wykonawca dokona cesji wierzytelności wynikających z niniejszej umowy na rzecz osób trzecich;

c) jeżeli w sytuacji zaistnienia przesłanek wymiany przedmiotu umowy na nowy wolny od wad, wymiana ta nie nastąpi w terminie 14 dni – w takiej sytuacji odstąpienie może nastąpić w odniesieniu do tego urządzenia, którego wada dotyczy.

6. Prawo do odstąpienia od umowy, o którym mowa w ust. 5, Zamawiający ma prawo zrealizować w terminie 14 dni od dnia powzięcia wiadomości o okoliczności stanowiącej podstawę odstąpienia od umowy. Odstąpienie nastąpi na piśmie z podaniem uzasadnienia.

7. Wykonawca ma prawo odstąpić od umowy wyłącznie z przyczyn leżących po jego stronie. Postanowienie ust. 6 stosuje się odpowiednio.

§ 6

1. Przedstawicielami upoważnionymi do realizacji umowy oraz nadzoru nad jej realizacją są:

a) ze strony Wykonawcy -; tel.:; e:mail:

b) ze strony Zamawiającego -; tel.:; e:mail:

2. Zamawiający informuje, że wymieniona do kontaktu osoba z ramienia Zamawiającego została poinformowana o fakcie jej wyznaczenia jako osoby do kontaktu.

§ 7

Zgodnie z art. 13 ust. 1 i 2 oraz art. 14 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), dalej RODO, informuję, że:



1. Administratorem danych osobowych przetwarzanych w w/w celach jest Instytut Agrofizyki im. Bohdana Dobrzańskiego Polskiej Akademii Nauk, ul. Doświadczalna 4, 20-290 Lublin, www.ipan.lublin.pl
2. Instytut – jako administrator danych – dołoży wszelkich starań, aby w jak najpełniejszym stopniu zrealizować wymogi Rozporządzenia i w ten sposób chronić Pani/Pana dane osobowe.
3. Nadzór nad prawidłowym przetwarzaniem danych osobowych w Instytucie sprawuje Inspektor Ochrony Danych, z którym można się kontaktować pod adresem e-mail: k.kajdrowicz@ipan.lublin.pl Dodatkowe dane osobowe Inspektora są dostępne na www.ipan.lublin.pl
4. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. C RODO w celu związanym z niniejszym postępowaniem o udzielenie zamówienia publicznego, a po zawarciu umowy również na podstawie art. 6 ust. 1 lit.b) RODO.
5. 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”;
6. 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, nie krótszy jednak niż cały czas trwania umowy
7. obowiązkiem 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;
8. w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
9. 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 (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);
 - 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 ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego);
 - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy 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.

§ 8

1. Zmiany postanowień umowy mogą wystąpić w następujących sytuacjach:

- a) zmiana obowiązujących, w dacie zawarcia umowy, przepisów, których regulacje wpływają na prawa i obowiązki Stron, jeżeli będzie konieczne dostosowanie treści umowy do aktualnego stanu prawnego;
- b) zmiana przepisów dotyczących podatku od towaru i usług;
- c) wprowadzenia nowej technologii i/lub zaprzestania produkcji produktów objętych umową, Zamawiający dopuszcza jego zastąpienie jedynie produktem równoważnym lub o wyższych parametrach jakościowych;
- d) wprowadzenia nowej technologii lub innych okoliczności pozwalających na obniżenie ceny przedmiotu umowy;
- e) wprowadzenia nowej technologii pozwalających na zastąpienie produktu o wyższej jakości niż w umowie przy zachowaniu ceny;
- f) konieczność zmiany osób przewidzianych do wzajemnego współdziałania lub wykonania przedmiotu umowy;
- g) wystąpienia zdarzeń siły wyższej jako zdarzenia zewnętrznego, niemożliwego do przewidzenia lub/i zapobieżenia;
- h) dopuszczalne będą inne zmiany umowy, o ile nie będą istotne w stosunku do treści oferty;
- i) dopuszcza się inne zmiany, o ile zachodzi co najmniej jedna z okoliczności zawartych w art. 144 ust. 1 ustawy Pzp;

2. Inicjatorem zmian może być Zamawiający lub Wykonawca poprzez pisemne wystąpienie w okresie obowiązywania umowy zawierające opis proponowanych zmian, ich uzasadnienie oraz termin wprowadzenia.

3. Wszelkie zmiany umowy wymagają zachowania formy pisemnej – w formie aneksu – pod rygorem ich nieważności.

§ 9

Zamawiający nie wyraża zgody na dokonywanie przez Wykonawcę cesji wierzytelności wynikających z niniejszej umowy na rzecz osób trzecich, w tym także w zakresie prawa do wynagrodzenia za przedmiot umowy.

§ 10

Umowa niniejsza podlega polskiemu prawu, a w sprawach w niej nie uregulowanych mają zastosowanie: ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2013 r., poz. 907 ze zm.) oraz Kodeks Cywilny, a w sprawach formalno – prawnych przepisy Kodeksu Postępowania Cywilnego.

§ 11

Wszelkie spory mogące wyniknąć w toku realizacji niniejszej umowy Strony poddają do rozpatrzenia Sądowi powszechnemu właściwemu dla siedziby Zamawiającego.

§ 12

Niniejsza umowa została sporządzona w dwóch jednobrzmiących egzemplarzach nie zawierających żadnych poprawek ani skreśleń, po jednym egzemplarzu dla każdej ze stron.

Integralną część umowy stanowi:

Załącznik nr 1 – SIWZ

Załącznik nr 2 – oferta Wykonawcy wraz zestawieniem wymaganych parametrów technicznych i użytkowych;

WYKONAWCA :

ZAMAWIAJĄCY:

UMOWA NR

W dniu2019 r. w Lublinie pomiędzy,
zwanym w treści umowy ZAMAWIAJĄCYM, reprezentowanym przez

1.

a działającą (-ym) na podstawie wpisu do pod numerem,
zwaną (-ym) w dalszej części umowy WYKONAWCĄ, reprezentowaną (-ym) przez:

1.

w wyniku postępowania o udzielenie zamówienia publicznego przeprowadzonego w trybie przetargu nieograniczonego na: dostawę laptopów z oprogramowaniem, licencji oraz akcesoriów komputerowych dla Instytutu Agrofizyki im. B. Dobrzańskiego Polskiej Akademii Nauk w Lublinie z podziałem na 14 części A-2401-9/2019

W części 1 i 8 Zamówienie finansowane z środków otrzymanych od Narodowego Centrum Badań i Rozwoju na realizację projektu: „Sonda profilowa TDT do pomiaru wilgotności, temperatury i elektrycznej przewodności gleby” (akronim: PROFILE-TDT) nr umowy STAIR/5/2016

W części 2; 3; 4; 6; 7; 10; 11; 12; 13; 14 Środki własne Instytutu Agrofizyki im. B. Dobrzańskiego Polskiej Akademii Nauk
W części 1; 5; 8 i 9 Zamówienie finansowane z środków otrzymanych od Narodowego Centrum Badań i Rozwoju na realizację projektu „Mobilny system iniekcyjnego, precyzyjnego nawadniania i nawożenia, zaspokajający indywidualne potrzeby rośliny” (Akronim: MSINiN), nr umowy: BIOSTRATEG3/343547/8/NCBR/2017)

została zawarta umowa o następującej treści:

§ 1

1. Wykonawca zobowiązuje się sprzedać, dostarczyć do siedziby Zamawiającego spełniający warunki określone w Specyfikacji Istotnych Warunków Zamówienia (SIWZ), stanowiącej załącznik nr 1 do niniejszej umowy oraz w złożonej ofercie i załączonym do niej zestawieniu wymaganych parametrów technicznych i użytkowych (oferta wraz z zestawieniem – załącznik nr 2 do umowy), zwane dalej przedmiotem umowy.
2. Koszty dostawy wraz z kosztami opakowania i ubezpieczenia ponosi Wykonawca.
3. Przedmiot umowy będzie dostarczony w opakowaniu zabezpieczonym przed uszkodzeniem w czasie transportu.
4. Wykonawca gwarantuje, iż przedmiot umowy jest fabrycznie nowy i nieużywany, ma należyłą jakość, funkcjonalność i parametry techniczne.

§ 2

1. Wykonanie umowy, tj. dostawa przedmiotu umowy nastąpi w terminie:

a) Dla części 7 i/lub 9 i/lub 13 i/lub 14 maksymalnie do dni kalendarzowych licząc od dnia podpisania umowy.*

b) Dla części 5 i/lub 6 i/lub 8 i/lub 12 maksymalnie do 14 dni kalendarzowych licząc od dnia podpisania umowy.*

* odpowiednie zostawić

2. Wykonawca jest zobowiązany zawiadomić Zamawiającego o gotowości dostawy przedmiotu umowy nie później niż na 1 dzień roboczy przed dostawą.

3. Po dostawie i przetestowaniu przedmiotu umowy Zamawiający dokona jego odbioru, który nastąpi poprzez podpisanie przez strony protokołu odbioru bez zastrzeżeń. Podpisanie protokołu odbioru z zastrzeżeniami wywołuje skutki równoznaczne ze zwłoką w wykonaniu umowy, jeżeli upłynął termin, o którym mowa w ust. 1.

§ 3

1. Na przedmiot umowy Wykonawca udziela gwarancji na okres wskazany w ofercie Wykonawcy wraz z zestawieniem wymaganych parametrów technicznych i użytkowych (załącznik nr 2 do umowy).

2. Gwarancja liczona jest od dnia podpisania bez zastrzeżeń protokołu odbioru przedmiotu umowy.

3. Gwarancja obejmuje wszystkie wykryte podczas eksploatacji przedmiotu umowy usterki i wady oraz uszkodzenia powstałe w czasie poprawnego, zgodnego z instrukcją jego użytkowania.

4. Serwis gwarancyjny świadczony będzie w miejscu użytkowania przedmiotu umowy. W przypadku niemożności dokonania naprawy na miejscu i konieczności dostarczenia przedmiotu umowy do punktu serwisowego wskazanego przez Wykonawcę – koszty dostarczenia do punktu serwisowego oraz z punktu serwisowego do miejsca siedziby Zamawiającego pokrywa Wykonawca.

5. Wykonawca przystąpi do usunięcia awarii – niezwłocznie po otrzymaniu informacji o awarii.

6. Wady ujawnione w okresie gwarancyjnym będą usunięte w terminie 14 dni od dnia ich zgłoszenia.

7. Jeżeli opóźnienie w naprawie przedmiotu umowy w stosunku do terminu określonego w ust. 6 przekroczy 14 dni Wykonawca zobowiązuje się do wymiany przedmiotu umowy na nowy, wolny od wad. Do momentu wymiany przedmiotu umowy Wykonawca pozostaje w opóźnieniu w usunięciu wad, chyba że wymiana nastąpiła w terminie określonym w ust. 6 w ramach usunięcia zgłoszonej wady.

8. Okres gwarancji ulega przedłużeniu o czas naprawy przedmiotu umowy, przy czym Zamawiający może dochodzić roszczeń z tytułu gwarancji także po jej upływie, jeżeli zgłoszenie wady miało miejsce przed jej upływem.

9. Zgłoszenia uszkodzeń będą przyjmowane drogą elektroniczną (e-mail), telefoniczną i faksową na nr we wszystkie dni robocze w godzinach 8.00 – 15.00.

10. W okresie gwarancji Zamawiający ma prawo do:

- dysponowania przedmiotem umowy.

11. Niezależnie od uprawnień z tytułu gwarancji, Zamawiający może wykonywać uprawnienia z tytułu rękojmi na zasadach ogólnych z tym, że okres rękojmi jest równy okresowi gwarancji.

12. Wykonawca zapewni na przedmiot umowy odpłatny serwis pogwarancyjny przez okres co najmniej 24 miesięcy od daty upływu terminu gwarancji, stosując średnie ceny z rynku polskiego.

§ 4

1. Za wykonanie umowy Wykonawca otrzyma wynagrodzenie w wysokości:

netto: (słownie:)

VAT: (słownie:)

Brutto: (słownie:)

2. Wynagrodzenie, o którym mowa w ust. 1 obejmuje wszelkie koszty związane z realizacją przedmiotu umowy w tym w szczególności koszt opakowania, dostarczenia, ubezpieczenia na czas transportu, świadczenia usług serwisu gwarancyjnego oraz wszelkie należne opłaty i podatki, w tym podatek VAT.

3. Wykonawca wystawi Zamawiającemu fakturę za przedmiot umowy po podpisaniu przez Strony bez zastrzeżeń protokołu odbioru.

4. Faktura, której załącznikiem będzie protokół odbioru, wystawiona będzie na,
NIP:

5. Po przedstawieniu przez Wykonawcę faktury wraz z załącznikiem, zgodnie z ust. 4, Zamawiający zapłaci należność wynikającą z tej faktury przelewem na konto Wykonawcy – w terminie 30 dni, licząc od daty jej doręczenia Zamawiającemu.

6. Przyjmuje się, że dniem zapłaty jest dzień obciążenia rachunku bankowego Zamawiającego.

§ 5

1. Wykonawca zapłaci Zamawiającemu kary umowne:

a) za zwłokę w wykonaniu umowy, tj. dostawie, zainstalowaniu, uruchomieniu przedmiotu umowy, w wysokości 0,4% wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy, za każdy dzień zwłoki, przy czym łączna kara umowna z tego tytułu nie może przekroczyć 10 % wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy;

b) za opóźnienie w usunięciu wad w stosunku do terminu określonego w § 3 ust. 6 umowy, w wysokości 0,4% wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy, za każdy dzień opóźnienia, przy czym łączna kara umowna z tego tytułu nie może przekroczyć 10 % wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy;

c) za odstąpienie od umowy przez Zamawiającego z przyczyn, za które ponosi odpowiedzialność Wykonawca, jak również za odstąpienie od umowy przez Wykonawcę z przyczyn leżących po jego stronie w wysokości 10% wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy.

2. Wykonawca wyraża zgodę na potrącenie kar umownych z przysługującego mu wynagrodzenia.
3. Zamawiający ma prawo dochodzić odszkodowania uzupełniającego na zasadach Kodeksu Cywilnego, jeżeli szkoda przewyższy wysokość kar umownych.
4. Wykonawcy od faktur niezapłaconych w terminie określonym w § 4 ust. 5 przysługują odsetki ustawowe.
5. Zamawiający ma prawo odstąpić od umowy ze skutkiem natychmiastowym z przyczyn, za które odpowiedzialność ponosi Wykonawca, w szczególności jeżeli:
 - a) zwłoka w wykonaniu umowy wynosi 14 dni, przy czym dostarczenie przedmiotu umowy w stanie niekompletnym, z wadą, niespełniającego wymagań określonych przez Zamawiającego wywołuje skutki równoznaczne ze zwłoką w jej wykonaniu, jeżeli upłynął termin, o którym mowa w § 2 ust. 1.
 - b) Wykonawca dokona cesji wierzytelności wynikających z niniejszej umowy na rzecz osób trzecich;
 - c) jeżeli w sytuacji zaistnienia przesłanek wymiany przedmiotu umowy na nowy wolny od wad, wymiana ta nie nastąpi w terminie 14 dni - w takiej sytuacji odstąpienie może nastąpić w odniesieniu do tego urzędnika, którego wada dotyczy.
6. Prawo do odstąpienia od umowy, o którym mowa w ust. 5, Zamawiający ma prawo zrealizować w terminie 14 dni od dnia powzięcia wiadomości o okoliczności stanowiącej podstawę odstąpienia od umowy. Odstąpienie nastąpi na piśmie z podaniem uzasadnienia.
7. Wykonawca ma prawo odstąpić od umowy wyłącznie z przyczyn leżących po jego stronie. Postanowienie ust. 6 stosuje się odpowiednio.

§ 6

1. Przedstawicielami upoważnionymi do realizacji umowy oraz nadzoru nad jej realizacją są:
 - a) ze strony Wykonawcy -; tel.:; e:mail:
 - b) ze strony Zamawiającego -; tel.:; e:mail:
2. Zamawiający informuje, że wymieniona do kontaktu osoba z ramienia Zamawiającego została poinformowana o fakcie jej wyznaczenia jako osoby do kontaktu.

§ 7

Zgodnie z art. 13 ust. 1 i 2 oraz art. 14 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), dalej RODO, informuję, że:

1. Administratorem danych osobowych przetwarzanych w w/w celach jest Instytut Agrofizyki im. Bohdana Dobrzańskiego Polskiej Akademii Nauk, ul. Doświadczalna 4, 20-290 Lublin, www.ipan.lublin.pl
2. Instytut – jako administrator danych - dołoży wszelkich starań, aby w jak najpełniejszym stopniu zrealizować wymogi Rozporządzenia i w ten sposób chronić Pani/Pana dane osobowe.

3. Nadzór nad prawidłowym przetwarzaniem danych osobowych w Instytucie sprawuje Inspektor Ochrony Danych, z którym można się kontaktować pod adresem e-mail: k.kajdrowicz@ipan.lublin.pl Dodatkowe dane osobowe Inspektora są dostępne na www.ipan.lublin.pl
4. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym postępowaniem o udzielenie zamówienia publicznego, a po zawarciu umowy również na podstawie art. 6 ust. 1 lit.b) RODO.
5. 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”;
6. 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, nie krótszy jednak niż cały czas trwania umowy
7. 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;
8. w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
9. 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 (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);
 - 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 ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego);
 - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy 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.

§ 8

1. Zmiany postanowień umowy mogą wystąpić w następujących sytuacjach:

- a) zmiana obowiązujących, w dacie zawarcia umowy, przepisów, których regulacje wpływają na prawa i obowiązki Stron, jeżeli będzie konieczne dostosowanie treści umowy do aktualnego stanu prawnego;
 - b) zmiana przepisów dotyczących podatku od towaru i usług;
 - c) wprowadzenia nowej technologii i/lub zaprzestania produkcji produktów objętych umową, Zamawiający dopuszcza jego zastąpienie jedynie produktem równoważnym lub o wyższych parametrach jakościowych;
 - d) wprowadzenia nowej technologii lub innych okoliczności pozwalających na obniżenie ceny przedmiotu umowy;
 - e) wprowadzenia nowej technologii pozwalających na zastąpienie produktu o wyższej jakości niż w umowie przy zachowaniu ceny;
 - f) konieczność zmiany osób przewidzianych do wzajemnego współdziałania lub wykonania przedmiotu umowy;
 - g) wystąpienia zdarzeń siły wyższej jako zdarzenia zewnętrznego, niemożliwego do przewidzenia lub/i zapobieżenia;
 - h) dopuszczalne będą inne zmiany umowy, o ile nie będą istotne w stosunku do treści oferty;
 - i) dopuszcza się inne zmiany, o ile zachodzi co najmniej jedna z okoliczności zawartych w art. 144 ust. 1 ustawy Pzp;
2. Inicjatorem zmian może być Zamawiający lub Wykonawca poprzez pisemne wystąpienie w okresie obowiązywania umowy zawierające opis proponowanych zmian, ich uzasadnienie oraz termin wprowadzenia.
3. Wszelkie zmiany umowy wymagają zachowania formy pisemnej - w formie aneksu - pod rygorem ich nieważności.

§ 9

Zamawiający nie wyraża zgody na dokonywanie przez Wykonawcę cesji wierzytelności wynikających z niniejszej umowy na rzecz osób trzecich, w tym także w zakresie prawa do wynagrodzenia za przedmiot umowy.

§ 10

Umowa niniejsza podlega polskiemu prawu, a w sprawach w niej nie uregulowanych mają zastosowanie: ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2013 r., poz. 907 ze zm.) oraz Kodeks Cywilny, a w sprawach formalno – prawnych przepisy Kodeksu Postępowania Cywilnego.

§ 11

Wszelkie spory mogące wyniknąć w toku realizacji niniejszej umowy Strony poddają do rozpatrzenia Sądowi powszechnemu właściwemu dla siedziby Zamawiającego.

§ 12

Niniejsza umowa została sporządzona w dwóch jednobrzmiących egzemplarzach nie zawierających żadnych poprawek ani skreśleń, po jednym egzemplarzu dla każdej ze stron.

Integralną część umowy stanowi:

Załącznik nr 1 – SIWZ

Załącznik nr 2 – oferta Wykonawcy wraz zestawieniem wymaganych parametrów technicznych i użytkowych;

WYKONAWCA :

ZAMAWIAJĄCY:

UMOWA NR

w dniu 2019 r. w Lublinie pomiędzy:

**Instytutem Agrofizyki im. Bohdana Dobrzańskiego Polskiej Akademii Nauk,
20-290 Lublin, ul. Doświadczalna 4**, reprezentowanym przez:

prof. dr hab. Cezary Sławiński – Dyrektor Instytutu

zwanym w dalszej części umowy **Zamawiającym**,

a działającą (-ym) na podstawie wpisu do pod numerem,
zwaną (-ym) w dalszej części umowy WYKONAWCĄ, reprezentowaną (-ym) przez:

1.

w wyniku postępowania o udzielenie zamówienia publicznego przeprowadzonego w trybie przetargu nieograniczonego na: dostawę laptopów z oprogramowaniem, licencji oraz akcesoriów komputerowych dla Instytutu Agrofizyki im. B. Dobrzańskiego Polskiej Akademii Nauk w Lublinie z podziałem na 14 części A-2401-9/2019

W części 1 i 8 Zamówienie finansowane z środków otrzymanych od Narodowego Centrum Badań i Rozwoju na realizację projektu: „Sonda profilowa TDT do pomiaru wilgotności, temperatury i elektrycznej konduktywności gleby” (akronim: PROFILE-TDT) nr umowy STAIR/5/2016

W części 2; 3; 4; 6; 7; 10; 11; 12; 13; 14 Środki własne Instytutu Agrofizyki im. B. Dobrzańskiego Polskiej Akademii Nauk
W części 1; 5; 8 i 9 Zamówienie finansowane z środków otrzymanych od Narodowego Centrum Badań i Rozwoju na realizację projektu „Mobilny system iniekcyjnego, precyzyjnego nawadniania i nawożenia, zaspokajający indywidualne potrzeby rośliny” (Akronim: MSINiN), nr umowy: BIOSTRATEG3/343547/8/NCBR/2017)

została zawarta umowa o następującej treści:

§ 1

1. Wykonawca zobowiązuje się sprzedać i dostarczyć do siedziby Zamawiającego spełniającą warunki określone w Specyfikacji Istotnych Warunków Zamówienia (SIWZ), stanowiącej załącznik nr 1 do niniejszej umowy oraz w złożonej ofercie i załączonym do niej zestawieniu wymaganych parametrów technicznych i użytkowych (oferta wraz z zestawieniem – załącznik nr 2 do umowy), zwane dalej przedmiotem umowy.
2. Wykonawca dostarczy przedmiot umowy wraz z instrukcją obsługi w języku polskim lub angielskim i dokumentami licencji udzielonej na czas nieoznaczony na oprogramowanie wskazane w opisie

przedmiotu umowy zawartym w SIWZ (załącznik nr 1 do umowy). Wykonawca oświadcza, że dysponuje prawem udzielenia licencji do tego oprogramowania.

3. Koszty dostawy wraz z kosztami opakowania i ubezpieczenia ponosi Wykonawca.
4. Oprogramowanie będzie dostępne w formie elektronicznej (download) z konta Administratora licencji w bazie producenta.
5. Wykonawca gwarantuje, iż przedmiot umowy jest fabrycznie nowy i nieużywany, ma należyłą jakość, funkcjonalność i parametry techniczne.

§ 2

1. Wykonanie umowy, tj. dostawa przedmiotu umowy nastąpi w terminie **dla części 2 i/lub 3 i/lub 4 i/lub 10 maksymalnie do dni kalendarzowych licząc od dnia podpisania umowy.**
2. Wykonawca jest zobowiązany zawiadomić Zamawiającego o gotowości dostawy przedmiotu umowy nie później niż na 1 dzień roboczy przed dostawą.
3. Po dostawie, zainstalowaniu, uruchomieniu i przetestowaniu przedmiotu umowy Zamawiający dokona jego odbioru, który nastąpi poprzez podpisanie przez strony protokołu odbioru bez zastrzeżeń. Podpisanie protokołu odbioru z zastrzeżeniami wywołuje skutki równoznaczne ze zwłoką w wykonaniu umowy, jeżeli upłynął termin, o którym mowa w ust. 1.

§ 3

1. Na przedmiot umowy Wykonawca udziela gwarancji na okres wskazany w ofercie Wykonawcy wraz z zestawieniem wymaganych parametrów technicznych i użytkowych (załącznik nr 2 do umowy).
2. Gwarancja liczona jest od dnia podpisania bez zastrzeżeń protokołu odbioru przedmiotu umowy.
3. Gwarancja obejmuje wszystkie wykryte podczas eksploatacji przedmiotu umowy usterki i wady oraz uszkodzenia powstałe w czasie poprawnego, zgodnego z instrukcją jego użytkowania.
4. Serwis gwarancyjny świadczony będzie w miejscu użytkowania przedmiotu umowy. W przypadku niemożności dokonania naprawy na miejscu i konieczności dostarczenia przedmiotu umowy do punktu serwisowego wskazanego przez Wykonawcę – koszty dostarczenia do punktu serwisowego oraz z punktu serwisowego do miejsca siedziby Zamawiającego pokrywa Wykonawca.
5. Wykonawca przystąpi do usunięcia awarii – niezwłocznie po otrzymaniu informacji o awarii.
6. Wady ujawnione w okresie gwarancyjnym będą usunięte w terminie 14 dni od dnia ich zgłoszenia.
7. Jeżeli opóźnienie w naprawie przedmiotu umowy w stosunku do terminu określonego w ust. 6 przekroczy 14 dni Wykonawca zobowiązuje się do wymiany przedmiotu umowy na nowy, wolny od wad. Do momentu wymiany przedmiotu umowy Wykonawca pozostaje w opóźnieniu w usunięciu wad, chyba że wymiana nastąpiła w terminie określonym w ust. 6 w ramach usunięcia zgłoszonej wady.

8. Okres gwarancji ulega przedłużeniu o czas naprawy przedmiotu umowy, przy czym Zamawiający może dochodzić roszczeń z tytułu gwarancji także po jej upływie, jeżeli zgłoszenie wady miało miejsce przed jej upływem.
9. Zgłoszenia uszkodzeń będą przyjmowane drogą elektroniczną (e-mail), telefoniczną i faksową na nr we wszystkie dni robocze w godzinach 8.00 – 15.00.
10. W okresie gwarancji Zamawiający ma prawo do:
 - dysponowania przedmiotem umowy.
11. Niezależnie od uprawnień z tytułu gwarancji, Zamawiający może wykonywać uprawnienia z tytułu rękojmi na zasadach ogólnych z tym, że okres rękojmi jest równy okresowi gwarancji.
12. Wykonawca zapewni na przedmiot umowy odpłatny serwis pogwarancyjny przez okres co najmniej 24 miesięcy od daty upływu terminu gwarancji, stosując średnie ceny z rynku polskiego.

§ 4

1. Za wykonanie umowy Wykonawca otrzyma wynagrodzenie w wysokości:
 - netto: zł. (słownie:)
 - VAT: zł. (słownie:)
 - Brutto: zł. (słownie:)**
2. Wynagrodzenie, o którym mowa w ust. 1 obejmuje wszelkie koszty związane z realizacją przedmiotu umowy w tym w szczególności koszt opakowania, dostarczenia, ubezpieczenia na czas transportu, świadczenia usług serwisu gwarancyjnego, koszt udzielenia licencji do oprogramowania oraz wszelkie należne opłaty i podatki, w tym podatek VAT.
3. Wykonawca wystawi Zamawiającemu fakturę za przedmiot umowy po podpisaniu przez Strony bez zastrzeżeń protokołu odbioru.
4. Faktura, której załącznikiem będzie protokół odbioru, wystawiona będzie na Instytut Agrofizyki im. B. Dobrzańskiego Polskiej Akademii Nauk, ul. Doświadczalna 4, 20-290 Lublin, NIP: 946-18-24-287.
5. Po przedstawieniu przez Wykonawcę faktury wraz z załącznikiem, zgodnie z ust. 4, Zamawiający zapłaci należność wynikającą z tej faktury przelewem na konto Wykonawcy – w terminie 30 dni, licząc od daty jej doręczenia Zamawiającemu.
6. Przyjmuje się, że dniem zapłaty jest dzień obciążenia rachunku bankowego Zamawiającego.

§ 5

1. Wykonawca zapłaci Zamawiającemu kary umowne:
 - a) za zwłokę w wykonaniu umowy, tj. dostawie, zainstalowaniu, uruchomieniu przedmiotu umowy, w wysokości 0,4% wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy, za każdy dzień zwłoki, przy czym łączna kara umowna z tego tytułu nie może przekroczyć 10 % wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy;

b) za opóźnienie w usunięciu wad w stosunku do terminu określonego w § 3 ust. 6 umowy, w wysokości 0,4% wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy, za każdy dzień opóźnienia, przy czym łączna kara umowna z tego tytułu nie może przekroczyć 10 % wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy;

c) za odstąpienie od umowy przez Zamawiającego z przyczyn, za które ponosi odpowiedzialność Wykonawca, jak również za odstąpienie od umowy przez Wykonawcę z przyczyn leżących po jego stronie w wysokości 10% wynagrodzenia brutto, o którym mowa w § 4 ust. 1 umowy.

2. Wykonawca wyraża zgodę na potrącenie kar umownych z przysługującego mu wynagrodzenia.

3. Zamawiający ma prawo dochodzić odszkodowania uzupełniającego na zasadach Kodeksu Cywilnego, jeżeli szkoda przewyższy wysokość kar umownych.

4. Wykonawcy od faktur niezapłaconych w terminie określonym w § 4 ust. 5 przysługują odsetki ustawowe.

5. Zamawiający ma prawo odstąpić od umowy ze skutkiem natychmiastowym z przyczyn, za które odpowiedzialność ponosi Wykonawca, w szczególności jeżeli:

a) zwłoka w wykonaniu umowy wynosi 14 dni, przy czym dostarczenie przedmiotu umowy w stanie niekompletnym, z wadą, niespełniającego wymagań określonych przez Zamawiającego wywołuje skutki równoznaczne ze zwłoką w jej wykonaniu, jeżeli upłynął termin, o którym mowa w § 2 ust. 1.

b) Wykonawca dokona cesji wierzytelności wynikających z niniejszej umowy na rzecz osób trzecich;

c) jeżeli w sytuacji zaistnienia przesłanek wymiany przedmiotu umowy na nowy wolny od wad, wymiana ta nie nastąpi w terminie 14 dni - w takiej sytuacji odstąpienie może nastąpić w odniesieniu do tego urządzenia, którego wada dotyczy.

6. Prawo do odstąpienia od umowy, o którym mowa w ust. 5, Zamawiający ma prawo zrealizować w terminie 14 dni od dnia powzięcia wiadomości o okoliczności stanowiącej podstawę odstąpienia od umowy. Odstąpienie nastąpi na piśmie z podaniem uzasadnienia.

§ 6

1. Przedstawicielami upoważnionymi do realizacji umowy oraz nadzoru nad jej realizacją są:

a) ze strony Wykonawcy –; tel.:; e:mail:

b) ze strony Zamawiającego –; tel.:; e:mail:

2. Zamawiający informuje, że wymieniona do kontaktu osoba z ramienia Zamawiającego została poinformowana o fakcie jej wyznaczenia jako osoby do kontaktu.

§ 7

Zgodnie z art. 13 ust. 1 i 2 oraz art. 14 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), dalej RODO, informuję, że:

1. Administratorem danych osobowych przetwarzanych w w/w celach jest Instytut Agrofizyki im. Bohdana Dobrzańskiego Polskiej Akademii Nauk, ul. Doświadczalna 4, 20-290 Lublin, www.ipan.lublin.pl
2. Instytut – jako administrator danych - dołoży wszelkich starań, aby w jak najpełniejszym stopniu zrealizować wymogi Rozporządzenia i w ten sposób chronić Pani/Pana dane osobowe.
3. Nadzór nad prawidłowym przetwarzaniem danych osobowych w Instytucie sprawuje Inspektor Ochrony Danych, z którym można się kontaktować pod adresem e-mail: k.kajdrowicz@ipan.lublin.pl Dodatkowe dane osobowe Inspektora są dostępne na www.ipan.lublin.pl
4. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym postępowaniem o udzielenie zamówienia publicznego, a po zawarciu umowy również na podstawie art. 6 ust. 1 lit.b) RODO.
5. 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”;
6. 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, nie krótszy jednak niż cały czas trwania umowy
7. 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;
8. w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
9. 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 (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);
 - 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 ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego);
 - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy 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.

§ 8

1. Zmiany postanowień umowy mogą wystąpić w następujących sytuacjach:

- a) zmiana obowiązujących, w dacie zawarcia umowy, przepisów, których regulacje wpływają na prawa i obowiązki Stron, jeżeli będzie konieczne dostosowanie treści umowy do aktualnego stanu prawnego;
- b) zmiana przepisów dotyczących podatku od towaru i usług;
- c) wprowadzenia nowej technologii i/lub zaprzestania produkcji produktów objętych umową, Zamawiający dopuszcza jego zastąpienie jedynie produktem równoważnym lub o wyższych parametrach jakościowych;
- d) wprowadzenia nowej technologii lub innych okoliczności pozwalających na obniżenie ceny przedmiotu umowy;
- e) wprowadzenia nowej technologii pozwalających na zastąpienie produktu o wyższej jakości niż w umowie przy zachowaniu ceny;
- f) konieczność zmiany osób przewidzianych do wzajemnego współdziałania lub wykonania przedmiotu umowy;
- g) wystąpienia zdarzeń siły wyższej jako zdarzenia zewnętrznego, niemożliwego do przewidzenia lub/i zapobieżenia;
- h) dopuszczalne będą inne zmiany umowy, o ile nie będą istotne w stosunku do treści oferty;
- i) dopuszcza się inne zmiany, o ile zachodzi co najmniej jedna z okoliczności zawartych w art. 144 ust. 1 ustawy Pzp;

2. Inicjatorem zmian może być Zamawiający lub Wykonawca poprzez pisemne wystąpienie w okresie obowiązywania umowy zawierające opis proponowanych zmian, ich uzasadnienie oraz termin wprowadzenia.

3. Wszelkie zmiany umowy wymagają zachowania formy pisemnej - w formie aneksu - pod rygorem ich nieważności.

§ 9

Zamawiający nie wyraża zgody na dokonywanie przez Wykonawcę cesji wierzytelności wynikających z niniejszej umowy na rzecz osób trzecich, w tym także w zakresie prawa do wynagrodzenia za przedmiot umowy.

§ 10

Umowa niniejsza podlega polskiemu prawu, a w sprawach w niej nie uregulowanych mają zastosowanie: ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2013 r., poz. 907 ze zm.) oraz Kodeks Cywilny, a w sprawach formalno – prawnych przepisy Kodeksu Postępowania Cywilnego.

§ 11

Wszelkie spory mogące wyniknąć w toku realizacji niniejszej umowy Strony poddają do rozpatrzenia Sądowi powszechnemu właściwemu dla siedziby Zamawiającego.

§ 12

Niniejsza umowa została sporządzona w dwóch jednobrzmiących egzemplarzach nie zawierających żadnych poprawek ani skreśleń, po jednym egzemplarzu dla każdej ze stron.

Integralną część umowy stanowi:

Załącznik nr 1 – SIWZ

Załącznik nr 2 – oferta Wykonawcy wraz zestawieniem wymaganych parametrów technicznych i użytkowych;

WYKONAWCA :

ZAMAWIAJĄCY:

Załącznik nr 6.1 do SIWZ

Zestawienie wymaganych parametrów technicznych i użytkowych – cz. 1

Część 1 – Dostawa komputerów PC laptopów – 9 szt.

1.1 Komputer PC laptop – 9 sztuk		
Producent:		
Model:		
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:	Oferowane – wypełnia Wykonawca:
Rodzaj laptopa	Wysoko wydajny ultrabook 14" Laptop wyposażony w oprogramowanie przeznaczone do: <ul style="list-style-type: none"> Specjalistycznego oprogramowania, obliczeń, edytora tekstu poczty elektronicznej 	
Procesor	Procesor taktowany zegarem co najmniej 1,6 GHz, pamięci cache 6 MB lub równoważny procesor klasy x64 zapewniający spełnienie poniższych kryteriów wydajności: <ul style="list-style-type: none"> - wydajność całego oferowanego systemu komputerowego min. 1914pkt w teście BAPCo MobileMark 2014. Test MobileMark 2014 Results powinien być wykonany w konfiguracji całego laptopa identycznej z wymaganą oraz przy rozdzielczości ekranu co najmniej 1920 x 1080 pikseli i innymi ustawieniami zgodnymi z zaleceniami producenta testu. 	
Pamięć RAM	8 GB 2133 MHz LPDDR3	
Dysk twardey	Dysk twardey zbudowany w oparciu o pamięć flash co najmniej 256 M.2 PCIe	
Karta graficzna	Zintegrowana z procesorem ze wsparciem dla DirectX 12	
Typ ekranu	14 cali, 1920 x 1080 (FullHD), matowy, bardzo szerokie kąty widzenia	
Urządzenie wskazujące	Zintegrowana funkcja klawiszy numerycznych	
Interfejsy komunikacyjne	Wi-Fi 802.11b/g/n/ac, Bluetooth,	
Złącza	Wyjścia: HDMI – 1 szt., USB 3.0 - 1 szt., USB Typu-C - 1 szt., USB 2.0 – 1 szt., zintegrowana kamera internetowa, czytnik kart pamięci MicroSD	
Wymiary	Waga max 1,2 kg, max. wysokość 16 mm	
Bateria	9 h pracy	
System operacyjny	Zainstalowany stabilny system operacyjny w języku polskim, zainstalowany na sprzęcie komputerowym objętym przedmiotem zamówienia przez producenta laptopa.	
Dołączone akcesoria	Dedykowane przez tego samego producenta co urządzenie firmowe etui na laptopa Dedykowana przez producenta przejściówka USB -> RJ-45 Zasilacz	

Dodatkowe informacje	<ul style="list-style-type: none"> • Białe podświetlenie klawiatury • Wielodotkowy, intuicyjny touchpad • Wbudowany czytnik linii papilarnych • Szyfrowanie TPM 	
Gwarancja na laptopa	12 miesięcy	

Załącznik nr 6.2 do SIWZ

Zestawienie wymaganych parametrów technicznych i użytkowych – cz. 2

Część 2 – Dostawa licencji na uaktualnienie systemu operacyjnego do wersji profesjonalnej (wersja edukacyjna)– 8 szt.

2.1 Licencja na uaktualnienie systemu operacyjnego do wersji profesjonalnej (wersja edukacyjna) – 8 sztuk		
Producent:		
Model:		
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:	Oferowane – wypełnia Wykonawca:
Upgrade	Licencja na podniesienie systemu operacyjnego do wersji profesjonalnej, edukacyjnej o następujących parametrach: w języku polskim, w pełni obsługujący pracę w domenie i kontrolę użytkowników w technologii ActiveDirectory, zcentralizowane zarządzanie oprogramowaniem i konfigurację systemu w technologii Group Policy.	
Wsparcie techniczne	12 miesięcy	

Załącznik nr 6.3 do SIWZ

Zestawienie wymaganych parametrów technicznych i użytkowych – cz. 3

Część 3 – Dostawa licencji na uaktualnienie systemu operacyjnego do wersji profesjonalnej EN (wersja edukacyjna)– 1 szt.

3.1 Licencja na uaktualnienie systemu operacyjnego do wersji profesjonalnej EN (wersja edukacyjna) – 1 sztuka		
Producent:		
Model:		
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:	Oferowane – wypełnia Wykonawca:
Upgrade	Licencja na podniesienie systemu operacyjnego do wersji profesjonalnej, edukacyjnej o następujących parametrach: w języku angielskim, w pełni obsługujący pracę w domenie i kontrolę użytkowników w technologii ActiveDirectory, zcentralizowane zarządzanie oprogramowaniem i konfigurację systemu w technologii Group Policy.	
Wsparcie techniczne	12 miesięcy	

Załącznik nr 6.4 do SIWZ

Zestawienie wymaganych parametrów technicznych i użytkowych – cz. 4

Część 4 – Dostawa Pakietu oprogramowania biurowego (wersja edukacyjna) – 13 szt.

4.1 Pakiet oprogramowania biurowego (wersja edukacyjna) – 13 sztuk		
Producent:		
Model:		
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:	Oferowane – wypełnia Wykonawca:
Opis	Najnowszy stabilny pakiet oprogramowania biurowe zawierające następujące elementy: procesor tekstu, arkusz kalkulacyjny, program do prezentacji, w pełni wspierający formaty plików .docx, .xlsx, .pptx, .accdb język polski zawierający aplikację służącą do obsługi poczty elektronicznej i organizacji czasu oraz umożliwiającą współpracę z serwerem przy pomocy protokołu dostępu MAPI/RPC. Zamawiający posiada edukacyjną grupową licencję oprogramowania Microsoft o numerze OPEN 98498763ZZE1911 lub równoważny spełniający powyższy opis.	
Wsparcie techniczne	12 miesięcy	



Załącznik nr 6.5 do SIWZ

Zestawienie wymaganych parametrów technicznych i użytkowych – cz. 5

Część 5 – Dostawa karty graficznej – 1 szt.

5.1 Karta graficzna – 1 sztuka		
Producent:		
Model:		
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:	Oferowane – wypełnia Wykonawca:
Rodzaj złącza	PCI-E X16 3.0	
Pamięć	3 GB DDR5	
Szyna pamięci	192-bit	
Taktowanie pamięci	8000 MHz	
Taktowanie rdzenia	1500 MHz	
Liczba rdzeni CUDA	1152	
Rodzaje wyjść	HDMI - 1 szt. DP – 3 szt. DVI – 1 szt.	
Chłodzenie	2 wentylatory	
Gwarancja	24 miesiące	

Załącznik nr 6.6 do SIWZ

**Zestawienie wymaganych parametrów technicznych i użytkowych – cz. 6
Część 6 – Dostawa dysku wewnętrznego SSD 250 GB– 2 szt.**

6.1 Dysk wewnętrzny SSD 250 – 2 sztuki		
Producent:		
Model:		
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:	Oferowane – wypełnia Wykonawca:
Pojemność	250 GB	
Format	2,5"	
Interfejs	SATA 6 Gb/s	
Prędkość odczytu	550 MB/s	
Prędkość zapisu	520 MB/s	
Odczyt losowy	98,000 IOPS	
Zapis losowy	90,000 IOPS	
MTBF (h)	1,500,000	
Gwarancja	24 miesiące	

Załącznik nr 6.7 do SIWZ

Zestawienie wymaganych parametrów technicznych i użytkowych – cz. 7

Część 7 – Dostawa pamięci RAM 4 GB – 1 szt.

7.1 Pamięć RAM – 1 sztuka		
Producent:		
Model:		
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:	Oferowane – wypełnia Wykonawca:
Pojemność	4GB	
Typ pamięci	DDR3	
Częstotliwość	1600MHz	
Inne	Pamięć RAM pozwalająca rozszerzyć funkcjonalność posiadanego komputera stacjonarnego lub równoważna pamięć RAM zgodna z powyższymi parametrami.	
Gwarancja	24 miesiące	

Załącznik nr 6.8 do SIWZ

Zestawienie wymaganych parametrów technicznych i użytkowych – cz. 8

Część 8 – Dostawa karty micro SD 256 GB – 10 szt.

8.1 Karta microSD 256 GB – 10 sztuk		
Producent:		
Model:		
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:	Oferowane – wypełnia Wykonawca:
Pojemność	256GB	
Interfejs	USB 3.0	
Prędkość odczytu	160 MB/s	
Prędkość zapisu	90 MB/s	
Gwarancja	36 miesięcy	

Załącznik nr 6.9 do SIWZ

Zestawienie wymaganych parametrów technicznych i użytkowych – cz. 9

Część 9 – Dostawa dysku wewnętrznego 500 GB –1 szt.

9.1 Dysk wewnętrzny SSD 500 GB – 1 sztuka		
Producent:		
Model:		
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:	Oferowane – wypełnia Wykonawca:
Zastosowanie	Dysk pasujący do laptopa ze złączem SSD M.2 PCIe	
Pojemność	500 GB	
Interfejs	PCI Express 3.0 x4 M.2	
Prędkość odczytu	3500 MB/s	
Prędkość zapisu	2500 MB/s	
MTBF (h)	1 500 000	
Gwarancja	36 miesięcy	

Załącznik nr 6.10 do SIWZ

Zestawienie wymaganych parametrów technicznych i użytkowych – cz. 10

Część 10 – Dostawa pakietu bezpieczeństwa antywirusowego przeznaczonego do ochrony komputerów – licencja – 250 szt., pakietu ochrony skrzynek pocztowych –licencja – 200 szt., pakietu ochrony urządzeń mobilnych –licencja – 5 szt.

10.1 Oprogramowanie antywirusowe		
Producent:		
Model:		
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:	Oferowane – wypełnia Wykonawca:
Wymagania użytkowe oprogramowania:	<p>Przedłużenie licencji programu posiadanego przez Zamawiającego na okres 36 miesięcy, składająca się z następujących pakietów:</p> <p>1.1. Ochrona stacji roboczych dla 250 stanowisk</p> <p>1.2. Ochrona skrzynek pocztowych dla 200 użytkowników</p> <p>1.3. Ochrona urządzeń mobilnych w ilości 5 sztuk</p> <p>Przedłużenie licencji na kolejny wymagany okres ma nastąpić z dniem 31.03.2019 r.</p>	
1.1 Pakiet bezpieczeństwa antywirusowego przeznaczony do ochrony komputerów		
Wymagania	<ol style="list-style-type: none"> Licencja na oprogramowanie do ochrony stacji roboczych dla 250 stanowisk. Pełne wsparcie dla systemu Windows Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10 Wsparcie dla 32- i 64-bitowej wersji systemu Windows. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives 	
Ochrona antywirusowa i antyspyware	<ol style="list-style-type: none"> Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. Wbudowana technologia do ochrony przed rootkitami. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. System ma oferować administratorowi możliwość 	



- definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
 9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótów w menu kontekstowym.
 10. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
 11. Możliwość skanowania dysków sieciowych i dysków przenośnych.
 12. Skanowanie plików spakowanych i skompresowanych.
 13. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
 14. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku ale również ma być możliwe użycie symbolu wieloznacznego „*” zastępującego dowolne znaki w ścieżce.
 15. Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik.
 16. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
 17. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
 18. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
 19. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
 20. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
 21. 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.
 22. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).



23. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
24. 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).
25. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
26. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
27. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
28. 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.
29. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
30. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
31. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
32. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
33. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
34. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
35. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
36. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
37. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
38. W przypadku gdy stacja robocza nie będzie



posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.

39. 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.
40. 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.
41. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
42. Możliwość wysłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
43. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
44. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
45. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
46. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
47. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
48. 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.
49. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykłe oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego



	<p>mechanizmu.</p> <p>50. 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.</p> <p>51. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.</p> <p>52. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.</p> <p>53. 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.</p> <p>54. 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.</p> <p>55. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły.</p> <p>56. 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.</p> <p>57. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.</p> <p>58. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.</p> <p>59. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika</p> <p>60. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).</p> <p>61. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:</p> <ul style="list-style-type: none">• tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,	
--	---	--



- tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
 - Tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.
62. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
63. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
64. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
65. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
66. 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.
67. 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.
68. 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.
69. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
70. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
71. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.
72. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
73. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http



74. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
75. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
76. Program ma być w pełni zgodny z technologią CISCO Network Access Control.
77. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.
78. 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.
79. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.
80. 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.
81. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
82. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.
83. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
84. Możliwość podejrzenia licencji za pomocą, której program został aktywowany.
85. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: ochrona antywirusowa i antyspyware, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, obsługa technologii Microsoft NAP.
86. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.
87. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.
88. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas po którym



	<p>automatycznie zostają przywrócone dotychczasowe ustawienia.</p> <p>89. Administrator ma możliwość wstrzymania polityk na 10 min, 30 min, 1 godzinę i 4 godziny</p> <p>90. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.</p> <p>91. Program musi posiadać opcję automatycznego skanowania komputera po dokonaniu zmian z użyciem opcji wstrzymania polityki.</p> <p>92. Aplikacja musi posiadać funkcję ręcznej aktualizacji komponentów programu.</p> <p>93. 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.</p> <p>94. Program musi posiadać możliwość definiowania stanów aplikacji, jakie będą wyświetlane użytkownikowi np. powiadomień o wyłączonych mechanizmach ochrony czy stanie licencji.</p> <p>95. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.</p> <p>96. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>97. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.</p> <p>98. Aplikacja musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.</p> <p>99. Administrator ma możliwość dodania wykluczenia na podstawie procesu, wskazującego bezpośrednio na określony plik wykonywalny.</p> <p>100. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania wybranej ścieżki, w której znajdują się pliki i foldery, które mają zostać wyłączone ze skanowania.</p> <p>101. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania obiektu co najmniej w oparciu o nazwę zagrożenia oraz jego lokalizację.</p> <p>102. Program musi oferować możliwość umieszczenia na liście wyłączeń ze skanowania pliku, wskazując sumę kontrolną pliku (jego HASH).</p> <p>103. Program musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”</p> <p>104. Program musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym</p>	
--	---	--



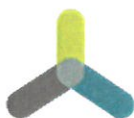
	<p>administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów.</p> <p>105. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.</p> <p>106. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.</p> <p>107. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.</p> <p>108. Administrator musi posiadać możliwość zastosowania reguł dla kontroli dostępu do stron w zależności od zdefiniowanego przedziału czasowego.</p> <p>109. Program musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”</p> <p>110. Program musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów.</p> <p>111. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.</p> <p>112. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.</p> <p>113. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.</p> <p>114. Administrator musi posiadać możliwość zastosowania reguł dla kontroli dostępu do stron w zależności od zdefiniowanego przedziału czasowego.</p>	
<p>Ochrona przed spamem</p>	<p>115. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.</p> <p>116. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.</p> <p>117. Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego.</p> <p>118. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.</p>	

	<p>119. 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.</p> <p>120. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam.</p> <p>121. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam.</p> <p>122. Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci” obecnym w programie Microsoft Outlook.</p> <p>123. 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”.</p> <p>124. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.</p>	
<p>Zapora osobista (personal firewall)</p>	<p>125. Zapora osobista ma pracować jednym z 4 trybów:</p> <ul style="list-style-type: none"> • tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora • tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo), • tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany, • tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji. <p>126. Program musi akceptować istniejące reguły w zaporze systemu Windows, zezwalające na ruch przychodzący.</p> <p>127. Możliwość tworzenia list sieci zaufanych</p> <p>128. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie</p> <p>129. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.</p> <p>130. Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym:</p>	



	<p>zezwól, zablokuj i pytaj o decyzję.</p> <p>131. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń.</p> <p>132. Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.</p> <p>133. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.</p> <p>134. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.</p> <p>135. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.</p> <p>136. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.</p> <p>137. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.</p> <p>138. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.</p> <p>139. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci</p> <p>140. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.</p> <p>141. 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.</p> <p>142. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6</p> <p>143. Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci.</p> <p>144. Program musi umożliwić ustalenie tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia.</p> <p>145. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem. Musi on działać w oparciu o:</p> <ul style="list-style-type: none">• rozwiązanie problemów z aplikacją lokalną którą wskazujemy z listy.• rozwiązywanie problemów z połączeniem z urządzeniem zdalnym na podstawie adresu IP.	
Kontrola dostępu do stron internetowych	<p>146. Aplikacja musi być wyposażony w zintegrowany moduł kontroli odwiedzanych stron</p>	

	<p>internetowych.</p> <p>147. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.</p> <p>148. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.</p> <p>149. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.</p> <p>150. Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i pod kategorii.</p> <p>151. Podstawowe kategorie w jakie aplikacja musi być wyposażony 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.</p> <p>152. Moduł musi posiadać także możliwość grupowania kategorii już istniejących.</p> <p>153. Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta.</p> <p>154. Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.</p> <p>155. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj.</p> <p>156. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny.</p>	
<p>Administracja zdalna</p>	<p>157. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2008 R2, 2012,2016 oraz systemach Linux.</p> <p>158. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).</p> <p>159. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.</p> <p>160. Konsola administracyjna musi umożliwiać podgląd szczegółów dotyczących bazy danych takich jak serwer Bazy danych, nazwę bazy danych, aktualny rozmiar bazy danych, nazwę hosta bazy danych</p> <p>161. Serwer administracyjny musi oferować możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych</p> <p>162. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika.</p> <p>163. Rozwiązanie ma być w pełni zgodne z</p>	



	<p>rozporządzeniem RODO</p> <p>164. 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.</p> <p>165. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.</p> <p>166. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.</p> <p>167. Konsola musi umożliwiać zarządzanie wszystkimi rozwiązaniami Producenta zabezpieczającymi przed zagrożeniami</p> <p>168. Konsola musi umożliwiać zarządzanie systemem dynamicznej ochrony przed zagrożeniami</p> <p>169. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.</p> <p>170. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.</p> <p>171. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.</p> <p>172. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.</p> <p>173. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.</p> <p>174. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.</p> <p>175. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie „hardware fingerprint”</p> <p>176. Serwer administracyjny musi oferować natywne wsparcie dla „VDI” oraz „Golden Master Image”</p> <p>177. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci.</p> <p>178. Instalacja serwera administracyjnego powinna oferować możliwość pracy w sieci rozproszonej nie wymagając dodatkowego serwera proxy.</p> <p>179. Rozwiązanie ma oferować możliwość komunikacji agenta przy wykorzystaniu http Proxy wbudowanego w serwer centralnego zarządzania bez wykorzystania dodatkowej maszyny Proxy</p> <p>180. Serwer musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.</p> <p>181. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.</p> <p>182. Serwer administracyjny musi oferować możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS</p> <p>183. Serwer administracyjny musi oferować</p>	
--	---	--



- możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP
184. Serwer administracyjny musi oferować możliwość konfiguracji polityk zabezpieczeń takich jak ograniczenia funkcjonalności urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11
 185. Serwer administracyjny musi oferować możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Map Google
 186. 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.
 187. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów.
 188. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
 189. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
 190. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows.
 191. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
 192. Centralna administracja musi pozwalać na zarządzanie urządzeniami mobilnymi z systemem iOS
 193. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
 194. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
 195. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
 196. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej.
 197. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów bazowych zarządzanego komputera oraz weryfikację zainstalowanego oprogramowania firm trzecich na stacji dla systemów Windows, Mac oraz Linux z możliwością jego odinstalowania
 198. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do



- serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
199. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego.
 200. Konsola ma oferować możliwość aktywacji oraz wdrożenie elementów systemu EDR producenta.
 201. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny.
 202. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
 203. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
 204. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
 205. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzeniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.
 206. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.
 207. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
 208. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
 209. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
 210. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
 211. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
 212. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko



	<p>do odczytu, odczyt/zapis.</p> <p>213. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.</p> <p>214. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego.</p> <p>215. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.</p> <p>216. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.</p> <p>217. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.</p> <p>218. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.</p> <p>219. 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.</p> <p>220. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji.</p> <p>221. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.</p> <p>222. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.</p> <p>223. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.</p> <p>224. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stację kliencką.</p> <p>225. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.</p> <p>226. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.</p> <p>227. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.</p> <p>228. Serwer administracyjny musi oferować możliwość utworzenia grup dynamicznych na podstawie zainstalowanego oprogramowania oraz zainstalowanych podzespołów bazowych w komputerach końcowych.</p>	
--	--	--



229. 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, podzespoły bazowe itp.
230. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.
231. 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.
232. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
233. 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.
234. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.
235. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta
236. Serwer administracyjny musi posiadać minimum 40 szablonów raportów przygotowanych przez producenta
237. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.
238. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
239. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.
240. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp.
241. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania oraz zapisania szablonów stworzonych filtrów
242. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.

- | | | |
|--|---|--|
| | <p>243. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostęp do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów.</p> <p>244. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.</p> <p>245. Serwer administracyjny musi oferować możliwość wygenerowania raportu na podstawie danych z systemu EDR producenta</p> <p>246. Serwer administracyjny musi oferować możliwość wygenerowania raportu na podstawie informacje o zainstalowanych podzespołów w stacjach roboczych</p> <p>247. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.</p> <p>248. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwić jego odświeżenie na żądanie.</p> <p>249. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.</p> <p>250. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.</p> <p>251. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.</p> <p>252. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.</p> <p>253. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień na zasadzie „WYSIWYG” z wykorzystaniem istniejących zmiennych</p> <p>254. Powiadomienia mailowe mają być wysłane w formacie HTML</p> <p>255. Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania.</p> <p>256. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.</p> <p>257. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.</p> <p>258. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.</p> <p>259. Serwer administracyjny musi oferować</p> | |
|--|---|--|



	<p>możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.</p> <p>260. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji bądź korzystając z powiązanego konta systemu zarządzania licencjami.</p> <p>261. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.</p> <p>262. W przypadku posiadania tylko jednej dodanej licencji do konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania</p> <p>263. Rozwiązanie ma oferować weryfikacji zainstalowanych komponentów bazowych urządzenia takich jak: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe, etc</p> <p>264. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.</p> <p>265. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia.</p> <p>266. Serwer administracyjny musi być wyposażony w mechanizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.</p> <p>267. W przypadku wystąpienia problemu rozwiązanie ma oferować możliwość przekierowania do wyszukiwarki Google z odwołaniem do konkretnego kodu błędu, który wystąpił w środowisku</p> <p>268. Serwer administracyjny oferować łatwy dostęp do zadań z poziomu menu kontekstowego w zależności od rodzaju urządzenia.</p> <p>269. Serwer administracyjny musi oferować aktualizację wszystkich komponentów z poziomu raportów jednym kliknięciem.</p> <p>270. Serwer administracyjny musi oferować możliwość konfiguracji listy adresów multicast</p> <p>271. Serwer administracyjny musi oferować WOL przy wykorzystaniu multicast</p> <p>272. Rozwiązanie ma oferować instalację agenta rozwiązania DLP producenta z poziomu jednego repozytorium.</p> <p>273. 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.</p> <p>274. Konfiguracja zestawów uprawnień musi umożliwiać przypisanie praw tylko do odczytu,</p>	
--	--	--

	<p>odczytu i użycia, oraz prawo do zapisania zmian w ramach danego zadania lub polityki w konsoli ERA.</p> <p>275. Rozwiązanie ma oferować zebrania logu diagnostycznego którego pobranie będzie możliwe z poziomu konsoli WEB</p> <p>276. Logi diagnostyczny, który można pobrać bezpośrednio z konsoli z modułów Anty SPM, firewall, HIPS, kontroli dostępu do urządzeń, kontroli dostępu do stron internetowych</p> <p>277. Logi diagnostyczne do pobrania z poziomu konsoli mają być dostępne 24h od daty ich wygenerowania</p> <p>278. Konsola webowa musi umożliwiać stronicowanie w widoku komputerów w celu ograniczenia liczby wyświetlanych maszyn na jednej stronie</p> <p>279. Konsola webowa musi umożliwiać weryfikację plików wysyłanych do serwerów producenta</p> <p>280. Konsola webowa musi umożliwiać zarządzanie systemem EDR producenta.</p> <p>281. Administrator musi mieć możliwość podłączenia do stacji roboczej z użyciem protokołu RDP bezpośrednio z poziomu konsoli ERA.</p> <p>282. Konsola administracyjna musi oferować możliwość weryfikacji zmian w produktach wprowadzanych przez producenta (Release notes dostępne bezpośrednio z konsoli zarządzania)</p> <p>283. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar</p> <p>284. Musi istnieć mechanizm, umożliwiający dodawanie reguł do istniejących już w module firewalla lub harmonogramie. Takie reguły można umieścić na początku lub końcu istniejącej listy.</p> <p>285. Administrator musi otrzymywać powiadomienia o dostępnych aktualizacjach z poziomu interfejsu Konsoli administracyjnej</p> <p>286. Konsola administracyjna musi umożliwiać dodanie własnego logotypu do interfejsu webowego.</p>	
--	--	--

10.2. Ochrona skrzynek pocztowych

Producent:

Model:

Nazwa podzespołu / parametry:	Opis minimalnych wymagań:	Oferowane – wypełnia Wykonawca:
Wymagania	<ol style="list-style-type: none"> Licencja na oprogramowanie do ochrony skrzynek pocztowych dla 200 użytkowników Skaner antywirusowy, antyspyware Możliwość skanowania wszystkimi modułami programu (heurystyka, sygnatury, adware/spyware, aplikacje niepożądane, aplikacje niebezpieczne) Skanowanie plików, plików spakowanych, archiwów samorozpakowujących, plików wiadomości e-mail 	



	<ol style="list-style-type: none">5. Konfiguracja wszystkich modułów oprogramowania (z wyjątkiem konfiguracji systemu antyspamowego) ma być możliwa poprzez edycję jednego pliku konfiguracyjnego6. Możliwość ustawień limitów dla modułu skanującego względem maksymalnego rozmiaru pliku, maksymalnej liczby warstw kompresji, maksymalnego rozmiaru archiwum, maksymalnego czasu skanowania, maksymalnego rozmiaru archiwum samorozpakowującego, rozszerzenia skanowanego pliku7. Możliwość tworzenia kwarantanny dla plików zainfekowanych w dowolnej lokalizacji w systemie plików8. Możliwość zdefiniowania częstotliwości aktualizacji programu z dokładnością do jednej minuty osobno dla aktualizacji sygnatur oraz osobno dla aktualizacji systemu antyspamowego9. Brak potrzeby instalacji dodatkowych zależności do systemu oprócz biblioteki LIBC, oprogramowanie po instalacji jest od razu gotowe do pracy10. Wbudowany bezpośrednio w program system obsługi plików spakowanych niewymagający zewnętrznych komponentów zainstalowanych w systemie11. Brak potrzeby instalacji źródeł jądra systemu oraz kompilacji jakichkolwiek modułów jądra do skanowania plików na żądanie12. Możliwość tworzenia przynajmniej pięciu poziomów dokładności czyszczenia zainfekowanych plików13. Możliwość zdefiniowania liczby wątków oraz liczby procesów dla każdego z modułów skanujących14. Możliwość tworzenia różnych akcji (przynajmniej 5-ciu różnych) w zależności od typu zdarzenia (w przypadku pliku nie przeskanowanego, pliku przeskanowanego, pliku zainfekowanego).15. Logowanie wykonanych akcji na plikach oraz zdarzeń dla poszczególnych modułów oprogramowania16. Wsparcie dla zewnętrznego serwera logującego syslog, możliwość definiowania dowolnego pliku logu (np. daemon, mail, user itp.)17. Możliwość zdefiniowania przynajmniej sześciu poziomów logowania programu18. Możliwość uruchomienia interfejsu programu dostępnego przez przeglądarkę Web19. Interfejs ma umożliwiać modyfikację ustawień programu oraz jego aktualizację a także przegląd statystyk dotychczas przeskanowanych plików20. Interfejs programu dostępny przez przeglądarkę Web wykorzystuje wbudowany w program serwer http21. Możliwość uruchomienia interfejsu Web na dowolnym porcie TCP22. Możliwość uruchomienia interfejsu Web na dowolnym interfejsie sieciowym23. Możliwość zabezpieczenia dostępu do interfejsu Web poprzez zdefiniowanie nazwy użytkownika i hasła24. Interfejs Web ma przedstawić administratorowi	
--	--	--



	<p>dokładny wynik skanowania poszczególnych plików w systemie wraz z możliwością pobrania tych wyników w postaci pliku tekstowego celem późniejszej analizy</p> <ol style="list-style-type: none">25. Możliwość podglądu informacji o licencji bezpośrednio z poziomu interfejsu Web, która zawiera przynajmniej informacje o liczbie dni do wygaśnięcia licencji, nazwę użytkownika licencji oraz pełną nazwę produktu, którego dotyczy licencja26. Program ma być wyposażony w graficzny menadżer kwarantanny dostępny z poziomu interfejsu Web. Menadżer ma oferować administratorowi możliwość przeglądu, pobrania, dodania i usunięcia plików w kwarantannie27. Menadżer kwarantanny ma posiadać możliwość wyszukiwania plików znajdujących się w kwarantannie przynajmniej po nazwie pliku, dodania pliku (możliwość definiowania przedziałów czasowych), rozmiarze (możliwość definiowania minimalnej i maksymalnej wielkości) oraz ilości plików (możliwość definiowania minimalnej i maksymalnej ilości)28. Interfejs Web do zarządzania produktem ma opierać się o wbudowane w program biblioteki PHP w wersji nie niższej niż 5.2.829. Interfejs dostępny poprzez przeglądarkę Web ma umożliwiać zarządzanie programem również wtedy, gdy przeglądarka nie obsługuje kodu JavaScript30. Możliwość stworzenia lokalnego repozytorium aktualizacji dla przynajmniej dwóch różnych produktów antywirusowych instalowanych na stacjach Windows31. Możliwość definicji użytkownika systemowego z prawami, którego zostanie uruchomiony demon skanujący32. Współpraca z mechanizmem automatycznej wysyłki podejrzanych plików do laboratorium producenta33. Wysyłka podejrzanych plików ma być możliwa bezpośrednio do producenta lub za pośrednictwem serwera zdalnego zarządzania34. Możliwość uaktywnienia dodatkowych funkcjonalności programu (moduł skanujący dla bramek sieciowych oraz moduł skanujący system plików), które nie wymagają od użytkownika instalacji dodatkowych zależności ani modułów a jedynie zacytowanie dodatkowych plików licencji35. Możliwość instalacji na dowolnym systemie Linux 2.6.x i nowszym.36. Producent ma dostarczyć pakiety instalacyjne w formacie RPM (dla dystrybucji Red Hat Mandriva, Suse oraz innych z nimi zgodnych), DEB (dla dystrybucji Debian, Ubuntu oraz innych z nimi zgodnych) oraz archiwum TGZ dla wszystkich pozostałych37. Możliwość instalacji na systemie FreeBSD 6.x, 7.x, 8.x i 9.x38. Wsparcie dla platform 32 oraz 64 bitowych39. Architektura programu umożliwia jego uruchomienie i optymalizację zarówno dla systemów jedno jak i wieloprocesorowych	
--	--	--



40. System ma mieć możliwość powiadomienia administratora o wykryciu infekcji oraz powiadomienia o zbliżającym się terminie wygaśnięcia licencji za pośrednictwem poczty e-mail.
41. Możliwość szybkiej konfiguracji oprogramowania poprzez skrypt powłoki. Skrypt umożliwi prostą konfigurację oprogramowania stosownie do wykrytego systemu operacyjnego, w jakim oprogramowanie zostało zainstalowane.
42. Skrypt ma mieć możliwość konfiguracji reguł firewala w taki sposób, aby przekierować niezbędne usługi do poszczególnych modułów programu.
43. Skrypt konfiguracyjny dla powłoki systemu ma zawierać funkcję przywrócenia wprowadzonych zmian regułach firewala
44. Możliwość skanowania ruchu SMTP, POP3, IMAP
45. Możliwość integracji z popularnymi systemami pocztowymi w tym przynajmniej z MTA Sendmail, Postfix, Exim, Qmail, Zmailer i CommuniGate Pro
46. Integracja z MTA ma zapewniać obustronne skanowanie ruchu pocztowego (ruchu przychodzącego oraz wychodzącego)
47. Możliwość integracji z dowolnym systemem MDA celem skanowania wyłącznie poczty przychodzącej do serwera
48. Możliwość pracy w trybie proxy SMTP celem skanowania wyłącznie poczty wychodzącej z serwera
49. Możliwość pracy w trybie proxy POP3 celem skanowania poczty pobieranej przez użytkowników z serwera POP3
50. Możliwość pracy w trybie proxy IMAP celem skanowania poczty pobieranej przez użytkowników z serwera IMAP
51. Możliwość współpracy z systemem AmaViS
52. Możliwość tworzenia różnych profili konfiguracji w zależności od adresu e-mail lub domeny osobno dla nadawców lub odbiorców wiadomości
53. Możliwość tworzenia białych i czarnych list domen i adresów e-mail
54. Wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty
55. Konfiguracja filtra antyspamowego ma znajdować się w innym pliku konfiguracyjnym niż konfiguracja skanera antywirusowego
56. Producent programu ma wyposażyć program w przynajmniej 5 predefiniowanych profili systemu antyspamowego
57. System antyspamowy ma być wyposażony przynajmniej sprawdzanie list RBL oraz mechanizm reputacji poczty.
58. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

10.3. Ochrona urządzeń mobilnych

Producent:

Model:

Nazwa parametru:	Opis minimalnych wymagań:	Oferowane – wypełnia Wykonawca:
Wymagania	<ol style="list-style-type: none"> 1. Licencja na oprogramowanie do ochrony urządzeń mobilnych w ilości 5 sztuk 2. Wspierany system co najmniej Android 4.0 (Ice Cream Sandwich) 3. Rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa. 4. Procesor: ARM (minimum ARMv7) 5. Pamięć wewnętrzna: 20 MB. 6. Połączenie z siecią Internet dla celów aktualizacji sygnatur i aktywacji licencji <p>Ochrona antywirusowa:</p> <ol style="list-style-type: none"> 7. Ochrona plików w czasie rzeczywistym 8. Ochrona przed atakami typu „phishing” 9. Skanowanie rozszerzeń DEX, bibliotek SO plików archiwum oraz innych. 10. Skanowanie dostępnego w urządzeniu nośnika pamięci SD. 11. Aplikacja musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne 12. Ochrona proaktywna wykrywająca nieznanne zagrożenia. 13. Aplikacja ma mieć możliwość określenia poziomu głębokości skanowania plików archiwum. 14. Aplikacja ma mieć możliwość określenia domyślnej akcji podejmowanej w przypadku wykrycia zagrożenia: przeniesienia do kwarantanny, usunięcia lub zignorowania. 15. W przypadku wykrycia zagrożenia użytkownik ma otrzymać odpowiednie powiadomienie 16. Aplikacja musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia 17. Aplikacja musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności, w pełni naładowane i podłączone do ładowarki <p>Skanowanie na żądanie:</p> <ol style="list-style-type: none"> 18. Aplikacja ma mieć możliwość skanowania zainstalowanych aplikacji. 19. Aplikacja ma wykorzystywać do celu skanowania metody heurystyczne wykrywające nieznanne zagrożenia. 20. Informacje o skanowaniu mają być przechowywane w plikach dziennika. 21. Użytkownik ma mieć możliwość wskazania akcji jaka ma być podjęta w przypadku wykrycia zagrożenia: poddania kwarantannie, usunięcia lub zignorowania. 22. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia, lub wskazania folderu, który ma być przeskanowany. 23. Aplikacja ma posiadać osobne dzienniki skanowania dla ochrony plików w czasie rzeczywistym, oraz skanowania na żądanie. <p>Filtr SMS/MMS i połączeń (jeśli system zezwala): Użytkownik musi mieć możliwość definiowania</p>	



	<p>własnych reguł dotyczących połączeń oraz wiadomości SMS/MMS bez konieczności podawania hasła administratora</p> <ol style="list-style-type: none">24. Reguły zdefiniowane przez administratora (w trybie administratora) muszą mieć wyższy priorytet niż reguły zdefiniowane przez użytkownika.25. Użytkownik i administrator ma mieć możliwość tworzenia białej i czarnej listy numerów telefonów.26. Użytkownik i administrator ma mieć możliwość dodania numeru telefonu, dla którego można określić akcje dla:<ol style="list-style-type: none">a. Przychodzącej wiadomości SMSb. Przychodzącej wiadomości MMSc. Połączenia wychodzącegod. Połączenia przychodzącego.27. Aplikacja ma mieć możliwość aktywacji blokady dla wszystkich połączeń oraz wiadomości SMS/MMS dla znanych kontaktów znajdujących się w książce telefonicznej urządzenia.28. Aplikacja ma mieć możliwość blokady połączeń telefonicznych oraz wiadomości SMS/MMS dla nieznanymi kontaktów (nieznajdujących się w książce telefonicznej urządzenia).29. Aplikacja ma mieć możliwość blokowania anonimowych połączeń przychodzących (pochodzących z ukrytych ID).30. Aplikacja ma być wyposażona w dziennik modułu antyspamowego zawierający informacje odnośnie filtrowania modułu. <p>Ochrona przed kradzieżą:</p> <ol style="list-style-type: none">31. Użytkownik ma mieć możliwość wprowadzenia zaufanej karty SIM.32. Dodanie zaufanej karty SIM ma się odbyć w oparciu o kartę wprowadzoną w danym urządzeniu lub w oparciu o dane wprowadzone ręcznie.33. Wprowadzenie danych ręcznie dotyczących zaufanej karty SIM ma się odbywać w oparciu o numer IMSI karty SIM.34. Aplikacja ma mieć możliwość wprowadzenia zaufanych odbiorców wiadomości, do których zostanie przesłana informacja w przypadku umieszczenia w urządzeniu innej niż zaufana karty SIM.35. Aplikacja ma mieć możliwość włączenia opcji ignorowania niedopasowania kart SIM.36. Użytkownik ma mieć możliwość edycji treści wiadomości SMS wysyłanej na zaufane numery telefonów w przypadku nie dopasowania karty SIM.37. W przypadku kradzieży urządzenia, prawowity użytkownik ma mieć możliwość wysłania na urządzenie komendy która umożliwi:<ol style="list-style-type: none">a. usunięcie zawartości urządzeniab. zablokowania urządzeniac. przesłania na zaufany numer telefonu lokalizacji GPS w której skradzione urządzenie się znajduje.38. Administrator musi mieć możliwość wysyłania powyższych komend bezpośrednio z poziomu	
--	---	--



	<p>konsoli centralnego zarządzania</p> <p>39. Możliwość zdalnego zresetowania hasła ma być możliwa tylko w przypadku wysłania odpowiedniego polecenia z zaufanego urządzenia</p> <p>Polityka ustawień: Aplikacja musi posiadać funkcjonalność pozwalającą administratorowi na monitorowanie ustawień urządzenia w celu weryfikacji czy są one zgodne z polityką.</p> <p>40. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia:</p> <ol style="list-style-type: none">Połączenie Wi-FiSatelity GPSUsługi lokalizacyjnePamięćRoaming danychRoaming połączeńNieznane źródłaTryb debugowaniaKomunikacja NFCSzyfrowanie pamięci masowej <p>41. Administrator ma mieć możliwość wyboru powyższych elementów</p> <p>Kontrola aplikacji:</p> <p>42. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji</p> <p>43. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji</p> <p>44. Blokowanie aplikacji musi być możliwe co najmniej za pomocą polityk:</p> <ol style="list-style-type: none">manualnego zdefiniowania listy blokowanych aplikacji na podstawie nazwyblokowanie na podstawie kategorii (np. kategorii Gry lub Społecznościowe)blokowanie na podstawie uprawnień aplikacji (np. aplikacji, które korzystają z modułu GPS do odczytania lokalizacji)blokowanie na podstawie źródła (np. aplikacje instalowane z innych źródeł niż sklep Google Play) <p>45. Administrator musi mieć możliwość monitorowania czasu, jaki użytkownik spędza na korzystaniu z poszczególnych aplikacji i sprawdzenia z jakich aplikacji użytkownik korzystał w ciągu ostatnich 30 dni, 7 dni oraz 24 godzin.</p> <p>Zabezpieczenia urządzenia:</p> <p>46. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej:</p> <ol style="list-style-type: none">minimalny poziom zabezpieczeń i złożoność blokady ekranumaksymalną dopuszczaną liczbę błędnych prób odblokowaniaodstęp czasu po którym użytkownik musi zmienić kod odblokowujący urządzenieczas przeznaczony na odblokowanie urządzeniaograniczyć dostęp do kamery wbudowanej w urządzenie	
--	---	--



	<p>Aktualizacje sygnatur:</p> <ol style="list-style-type: none">47. Wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.48. Aplikacja ma mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje sygnatur co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin.49. Aplikacja ma mieć funkcjonalność ochrony hasłem wybranych modułów ochrony, w tym co najmniej dostępu do ustawień ochrony antywirusowej, ustawień modułu antyspamowego, ochrony przed kradzieżą, uruchamiania zadań audytu zabezpieczeń oraz przed deinstalacją.50. Aplikacja ma mieć możliwość ukrycia ikony powiadomień. <p>Konfiguracja i zdalne zarządzanie:</p> <ol style="list-style-type: none">51. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne52. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją53. Administrator musi mieć możliwość zdalnego wysyłania komunikatów z poziomu konsoli centralnego zarządzania do użytkowników urządzeń mobilnych54. Przesłana wiadomość musi wyświetlać się w formie wyskakującego okna, aby użytkownik ich nie przeoczył55. Administrator musi mieć możliwość kontrolowania mechanizmu aktualizacji oprogramowania	
--	---	--

Załącznik nr 6.11 do SIWZ

Zestawienie wymaganych parametrów technicznych i użytkowych – cz. 11

Część 11 – Dostawa komputerów stacjonarnych – 4 szt.

11.1 Komputer biurowy z system operacyjnym - 4 sztuki		
Producent:		
Model:		
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:	Oferowane – wypełnia Wykonawca:
Typ	Komputer stacjonarny wykonany przez jednego producenta. W ofercie wymagane jest podanie modelu, symbolu oraz producenta podzespołów komputera	
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb przetwarzania aplikacji biurowych, aplikacji edukacyjnych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych.	
Wydajność obliczeniowa	Procesor taktowany zegarem co najmniej 2,8 GHz, pamięci cache 9 MB lub równoważny procesor klasy x86 zapewniający spełnienie poniższych kryteriów wydajności: - wydajność całego oferowanego systemu komputerowego min. 1115 pkt w teście BAPCo SYSMark 2014 . Test SYSMark 2014 Results powinien być wykonany w konfiguracji całego komputera identycznej z wymaganą oraz przy rozdzielczości ekranu co najmniej 1920 x 1080 pikseli i innymi ustawieniami zgodnymi z zaleceniami producenta testu.	
Pamięć operacyjna	8GB 2400 MHz możliwość rozbudowy do min 32 GB	
Parametry pamięci masowej	Zbudowana w oparciu o pamięć flash co najmniej 500 GB SSD	
Wydajność grafiki	Grafika zintegrowana z procesorem powinna umożliwiać pracę na 2 monitorach ze wsparciem dla DirectX 12, Open CL 2.0, OpenGL 4.4 – z możliwością dynamicznego przydzielenia pamięci 1,7 GB.	
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, porty słuchawek i mikrofonu na przednim oraz na tylnym panelu obudowy	

Obudowa	<p>Miejsca na wewnętrzne dyski/napędy: 2 x 3,5", 1 x 2,5", Miejsca na zewnętrzne dyski/napędy: 1 x 3,5" 2 x 5,25", Wyprowadzone złącza Wejście mikrofonowe - 1 szt., Wyjście słuchawkowe/głośnikowe - 1 szt., USB 3.0 - 2 szt., USB 2.0 - 2 szt. Zasilacz o mocy minimum 210 W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85%, przy 50% obciążeniu.</p>	
Ergonomia	<p>Suma wymiarów obudowy (wysokość + szerokość + głębokość mierzona po krawędziach zewnętrznych) nie może wynosić więcej niż 860 mm</p>	
Wymagania dodatkowe	<p>Licencja najnowszego systemu operacyjnego. Stabilny system operacyjny w języku polskim, w pełni obsługujący pracę w domenie i kontrolę użytkowników w technologii ActiveDirectory, zcentralizowane zarządzanie poprogramowaniem i konfigurację systemu w technologii Group Policy. System operacyjny, zainstalowany na sprzęcie komputerowym objętym przedmiotem zamówienia. Dołączony nośnik z oprogramowaniem, sterownikami, płyty Recovery umożliwiające instalacje systemu w wersji 64 bitowej.</p>	



interfejs	<p>Wbudowane porty i złącza w płyci głównej: Wbudowane porty minimalnie:</p> <ul style="list-style-type: none">- 1 x DVI- 1 x DP- 1 x RJ-45- 1 x PCI-E 3.0 16x- 2 x PCI-E 1x- 6.x USB 2.0- 4x Złącza USB 3.0 <p>Dodatkowe informacje o portach USB 2.0/3.0/3.1</p> <ul style="list-style-type: none">- 2 x USB 3.0 (przedni panel)- 2 x USB 3.0 (tylny panel)- 2 x USB 2.0 (przedni panel)- 2 x USB 2.0 (tylny panel)- 2 x USB 2.0 (wewnątrz)- 3 x Serial ATA	
Poziom hałasu	W tryb pracy: 50% obciążenie procesora - 22 dB (osoba obsługująca)	
Wymagania dodatkowe	Nagrywarka DVD +/-RW, klawiatura, mysz	
Gwarancja komputera	24 miesiące	

Załącznik nr 6.12 do SIWZ
Zestawienie wymaganych parametrów technicznych i użytkowych – cz. 12
Część 12 – Dostawa monitorów 24 cale – 5 szt.

12.1 Monitor 24 cale – 5 sztuk		
Producent:		
Model:		
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:	Oferowane – wypełnia Wykonawca:
Typ ekranu	Płasko ekranowy monitor panoramiczny LED, IPS 24”, przeciwoodblaskowa powłoka (matowa)	
Jasność	300 cd/m ²	
Kontrast	1000 :1 (typowy) 2 000 000 :1 (dynamiczny)	
Wielkość plamki	0,27 mm	
Kąty widzenia (pion/poziom)	178°/178°	
Czas reakcji matrycy	8 ms	
Kolory	16.7mln	
Rozdzielczość maksymalna	1920 x 1200	
Ustawienia ekranu w pionie i poziomie	Pivot	
Złącze	VGA – 1 szt., DVI-D - 1 szt., Display Port - 1 szt., USB 2.0 – 4 szt.	
Średnie użycie energii	Pobór prądu w trybie uśpienia-poniżej 0,5 W	
Podstawa	kompatybilność z VESA 100mm	
Normy i standardy	Monitory muszą być wykonane zgodnie normami i posiadać Certyfikaty: TCO 5.0, EPEAT Gold, Energy Star 5.1	
Gwarancja	36 miesięcy	

Zestawienie wymaganych parametrów technicznych i użytkowych – cz. 13

Część 13 – Dostawa listwy głośnikowej dedykowanej do monitora – 5 szt.

13.1 Listwa głośnikowa dedykowana do monitora – 5 sztuk		
Producent:		
Model:		
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:	Oferowane – wypełnia Wykonawca:
Zastosowanie	Oryginalne głośniki tego samego producenta co monitory posiadane przez Zamawiającego. Modele posiadanych monitorów to 2412M. Głośnik wyposażony jest w odpowiednie uchwyty.	
Moc	2 x 5 W na kanał	
Gniazda słuchawkowe	2 szt.	
Zasilanie	12 V prądu stałego	
Gwarancja	12 miesięcy	

Załącznik nr 6.14 do SIWZ

Zestawienie wymaganych parametrów technicznych i użytkowych – cz. 14

Część 14 – Dostawa zestawów „klawiatura i mysz bezprzewodowa” – 7 szt.

14.1 Zestaw klawiatura i mysz bezprzewodowa – 7 sztuk		
Producent:		
Model:		
Nazwa podzespołu / parametry:	Opis minimalnych wymagań:	Oferowane – wypełnia Wykonawca:
Łączność	bezprzewodowa	
Interfejs	2,4 GHz, USB (nanoodbiornik)	
Klawiatura	Klawisze - cicha praca, małym skokiem, multimedialne, funkcyjne, podpórka pod nadgarstki, wyłącznik na przednim panelu klawiatury.	
Mysz	Sensor – optyczny, 3 przyciski, rolka przewijania, rozdzielczość-1000dpi	
Technologia czujnika:	Zaawansowane śledzenie optyczne	
Gwarancja	24 miesiące	