WUPXXV/2/3321/11/2015

## SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

do postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego,
o wartości zamówienia mniejszej niż kwoty określone w przepisach wydanych na podstawie
art.11 ust. 8 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych na:

**Dostawa sprzętu komputerowego i oprogramowania
dla Wojewódzkiego Urzędu Pracy w Poznaniu**

**październik 2015 r.**

1. **Nazwa oraz adres Zamawiającego.**

**WOJEWÓDZKI URZĄD PRACY W POZNANIU**

ul. Kościelna 37

60-537 Poznań

wuppoznan.praca.gov.pl

NIP: 778-13-79-161

1. **Tryb udzielenia zamówienia.**
2. Postępowanie prowadzone jest w trybie przetargu nieograniczonego, o wartości mniejszej niż wartości określone na podstawie art. 11 ust. 8, zgodnie z przepisami ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych, zwanej w dalszej części specyfikacji „ustawą Pzp” (tj. Dz. U. z 2013 r., poz. 907 ze zm.).
3. Postępowanie prowadzone jest przez komisję przetargową, powołaną
do przeprowadzenia niniejszego postępowania o udzielenie zamówienia publicznego.
4. Do czynności podejmowanych przez Zamawiającego i Wykonawców w postępowaniu
o udzielenie zamówienia, stosuje się przepisy powołanej ustawy Pzp oraz aktów wykonawczych wydanych na jej podstawie, a w sprawach nieuregulowanych, przepisy ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (t.j. Dz. U. z 2014 r., poz. 121 ze zm.) i inne obowiązujące akty prawne.
5. **Opis przedmiotu zamówienia.**
6. Przedmiotem zamówienia jest dostawa sprzętu komputerowego i oprogramowania
dla Wojewódzkiego Urzędu Pracy w Poznaniu.
7. Zamówienie zostało podzielone na 2 części, Zamawiający dopuszcza możliwość składania ofert częściowych, z których każda stanowi odrębną część przedmiotu zamówienia:

**Część 1**

1. Zakup zestawów komputerowych wraz z oprogramowaniem – 16 szt.
2. Aktualizacja i rozszerzenie oprogramowania antywirusowego na stacje robocze
i serwery wraz z konsolą do centralnej administracji:
3. aktualizacje - 310 szt.,
4. nowe licencje – 7 szt.
5. Program do zdalnej kontroli i zdalnego współdzielenia pulpitu przez internet – 1 szt.

**Część 2**

* + 1. Zakup i wdrożenie Forti Analyzer 200D.
		2. Odnowienie licencji i przedłużenie usług Vmware.
1. Szczegółowy opis przedmiotu zamówienia został określony w załączniku nr 1 stanowiącym integralną część SIWZ.
2. Zamawiający w załączniku nr 1 do SIWZ wymaga podania wartości parametrów technicznych oferowanego sprzętu komputerowego – dotyczy części 1 pkt 1.
3. Oznaczenie przedmiotu zamówienia według kodu CPV:

Nazwa: Urządzenia komputerowe Kod: 30 20 00 00 – 1

Nazwa: Pakiety oprogramowania i systemy informatyczne Kod: 48 00 00 00 – 8

1. **Termin wykonania zamówienia.**

**Część 1**

1. w terminie do 21 dni kalendarzowych od daty podpisania umowy,
2. od dnia 19.11.2015 r. na okres 12 miesięcy,
3. od dnia 22.11.2015 r. na okres 12 miesięcy.

**Część 2**

1. w terminie do 21 dni kalendarzowych od daty podpisania umowy,
2. od daty podpisania umowy do 13.10.2018 r.
3. **Warunki udziału w postępowaniu i opis sposobu dokonywania oceny spełnienia tych warunków.**
4. W postępowaniu mogą wziąć udział Wykonawcy, którzy spełniają warunki udziału
w postępowaniu, o których mowa w art. 22 ust. 1 ustawy Pzp:
	1. posiadają uprawnienia do wykonywania określonej działalności lub czynności,
	jeżeli przepisy prawa nakładają obowiązek ich posiadania,
	2. posiadają wiedzę i doświadczenie;

Zamawiający uzna, że Wykonawca spełnia ten warunek, jeśli wykaże, że w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonuje (tylko w przypadku świadczeń okresowych lub ciągłych) lub wykonał należycie co najmniej:
dla **części 1**: 2 dostawy polegające na dostawie sprzętu komputerowego
i oprogramowania o wartości minimum 40 000,00 zł brutto każda,
dla **części 2**: 2 dostawy urządzeń do zapisywania zdarzeń i raportowania
o wartości minimum 20 000,00 zł brutto każda,

oraz załączy dowody potwierdzające, że dostawy te zostały wykonane lub są wykonywane należycie;

* 1. dysponują odpowiednim potencjałem technicznym oraz osobami zdolnymi
	do wykonania zamówienia;

Zamawiający uzna, że Wykonawca spełnia ten warunek, jeśli wykaże, że dysponuje co najmniej dwoma akredytowanymi inżynierami, których kwalifikacje potwierdzone będą certyfikatami producenta systemów raportowania i logowania – dot. **części 2**.

* 1. znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.
1. Wykonawca może polegać na wiedzy i doświadczeniu innych podmiotów, osobach zdolnych do wykonania zamówienia, niezależnie od charakteru prawnego łączących go
z nimi stosunków.
2. Podmiot, który zobowiązał się do udostępnienia zasobów zgodnie z art. 26
ust. 2b ustawy Pzp, odpowiada solidarnie z wykonawcą za szkodę zamawiającego powstałą wskutek nieudostępnienia tych zasobów, chyba że za nieudostępnienie zasobów nie ponosi winy.
3. W postępowaniu mogą wziąć udział Wykonawcy, którzy nie podlegają wykluczeniu
z postępowania o udzielenie zamówienia publicznego w okolicznościach, o których mowa w art. 24 ust. 1 ustawy Pzp.
4. Zamawiający dokona oceny spełnienia warunków na podstawie złożonych dokumentów
i oświadczeń opisanych w rozdziale VI SIWZ, według formuły „spełnia/nie spełnia”.
5. **Oświadczenia i dokumenty, jakie mają dostarczyć Wykonawcy w celu potwierdzenia spełnienia warunków udziału w postępowaniu.**
6. Na potwierdzenie spełniania warunków udziału w postępowaniu, określonych
w rozdz. V ust. 1 specyfikacji, Wykonawcy muszą przedstawić następujące dokumenty:
	1. oświadczenie Wykonawcy o spełnieniu warunków określonych w art. 22 ust 1 ustawy Pzp, według wzoru stanowiącego załącznik nr 3 do SIWZ,
	2. wykaz wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, głównych usług, w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia jest krótszy – w tym okresie,
	z podaniem ich wartości, przedmiotu, daty wykonania i podmiotów, na rzecz których usługi zostały wykonane, oraz załączeniem dowodów, czy zostały wykonane lub są wykonywane należycie według wzoru stanowiącego załącznik
	nr 6do SIWZ.
	3. wykaz osób, które będą uczestniczyć w wykonywaniu zamówienia,
	w szczególności odpowiedzialnych za świadczenie usługi, wraz z informacjami
	na temat ich kwalifikacji zawodowych, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia, a także zakresu wykonywanych przez nie czynności, oraz informacją o podstawie do dysponowania tymi osobami – według wzoru stanowiącego załącznik nr 7 do SIWZ.
	4. Jeżeli Wykonawca, wykazując spełnienie warunków, o których mowa w art. 22
	ust. 1 ustawy Pzp, polega na zasobach innych podmiotów na zasadach określonych w art. 26 ust. 2b ustawy Pzp:
		1. zobowiązany jest udowodnić Zamawiającemu, iż będzie dysponował tymi zasobami w trakcie realizacji zamówienia, w szczególności przedstawiając w tym celu pisemne zobowiązanie tych podmiotów (w formie oryginału)
		do oddania mu do dyspozycji niezbędnych zasobów na potrzeby wykonania zamówienia,
		2. W celu oceny, czy Wykonawca będzie dysponował zasobami innych podmiotów w stopniu niezbędnym dla należytego wykonania zamówienia oraz oceny, czy stosunek łączący Wykonawcę z tymi podmiotami gwarantuje rzeczywisty dostęp do ich zasobów, Zamawiający żąda
		w zakresie pkt 1.2 i 1.3 niniejszego ustępu dokumentów dotyczących
		w szczególności:
			1. zakresu dostępnych Wykonawcy zasobów innego podmiotu,
			2. sposobu wykorzystania zasobów innego podmiotu przez Wykonawcę przy wykonywaniu zamówienia,
			3. charakteru stosunku, jaki będzie łączył Wykonawcę z innymi podmiotami,
			4. zakresu i okresu udziału innego podmiotu przy wykonywaniu zamówienia.

2. W celu wykazania braku podstaw do wykluczenia z postępowania o udzielenie zamówienia w okolicznościach, o których mowa w art. 24 ust. 1 ustawy Pzp, Wykonawcy muszą przedstawić następujące dokumenty:

* 1. Oświadczenie Wykonawcy o braku podstaw do wykluczenia, według wzoru stanowiącego załącznik nr 4 do SIWZ.
	2. Aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji
	o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 1 pkt 2 ustawy Pzp (wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert).
	3. Aktualne na dzień składania ofert zaświadczenie właściwego naczelnika Urzędu Skarbowego, potwierdzające, że Wykonawca nie zalega z opłacaniem podatków lub zaświadczenia, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności, lub wstrzymanie w całości wykonania decyzji właściwego organu (wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert).
1. Jeżeli Wykonawca, wykazując spełnienie warunków o których mowa w art. 22 ust. 1 ustawy, polega na zasobach innych podmiotów na zasadach określonych w art.
26 ust. 2b ustawy Pzp, a podmioty te będą brały udział w realizacji części zamówienia, przedkłada także dokumenty dotyczące tego podmiotu w zakresie wymaganym dla Wykonawcy, określone w ust. 2 pkt 2.1. - 2.3 niniejszego rozdziału.
2. W celu potwierdzenia, że oferowana dostawa odpowiada wymaganiom określonym przez Zamawiającego, Wykonawca musi przedstawić następujący dokument:
* aktualny certyfikat ISO 27001 lub równoważny - dot. **części 2**.
1. Wykonawca wraz z ofertą składa listę podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 ustawy Pzp, albo informację o tym, że nie należy do grupy kapitałowej, według wzoru stanowiącego załącznik nr 5 do SIWZ.
2. W przypadku oferty składanej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, dokumenty i oświadczenia wymienione w ust. 2 i 4 niniejszego rozdziału SIWZ, składa każdy z Wykonawców oddzielnie. Dokumenty, o których mowa
w ust. 1 niniejszego rozdziału składane są wspólnie przez Wykonawców.
3. W przypadku, gdy Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium RP, w miejsce dokumentów, o których mowa w ust. 2 pkt 2.2 i pkt 2.3 niniejszego rozdziału, zobowiązany jest przedłożyć dokument lub dokumenty, wystawione w kraju,
w którym ma siedzibę lub miejsce zamieszkania, potwierdzające, że:
	1. nie otwarto jego likwidacji ani nie ogłoszono upadłości, (wystawione nie wcześniej
	niż 6 miesięcy przed upływem terminu składania ofert);
	2. nie zalega z uiszczaniem podatków, opłat albo że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie
	w całości wykonania decyzji właściwego organu (wystawione nie wcześniej
	niż 3 miesiące przed upływem terminu składania ofert);
4. Jeżeli w kraju miejsca zamieszkania osoby lub w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się powyższych dokumentów, Wykonawca może je zastąpić stosownym dokumentem, zawierającym oświadczenie,
w którym określa się także osoby uprawnione do reprezentacji Wykonawcy, złożone przed właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego odpowiednio kraju miejsca zamieszkania osoby lub kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, lub przed notariuszem. Powyższe dokumenty muszą być wystawione w terminach odpowiednich do rodzaju dokumentów, o których mowa w ust. 6 pkt 6.1 i 6.2 niniejszego rozdziału.
5. W przypadku wątpliwości co do treści dokumentu złożonego przez Wykonawcę mającego siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, Zamawiający może zwrócić się do właściwych organów odpowiednio kraju miejsca zamieszkania osoby lub kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, z wnioskiem o udzielenie niezbędnych informacji dotyczących przedłożonego dokumentu.
6. Z treści załączonych dokumentów musi wynikać jednoznacznie, iż Wykonawca spełnił warunki udziału w postępowaniu.
7. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
8. Dokumenty, o których mowa w rozdziale VI specyfikacji, należy przedstawić w formie oryginałów lub kopii, poświadczonych za zgodność z oryginałem przez osobę/y uprawnioną/e do reprezentowania Wykonawcy, z wyłączeniem dokumentu, o którym mowa w ust. 1 pkt 1.4.1 niniejszego rozdziału, który należy przedstawić w formie oryginału.
9. Zamawiający może zażądać przedstawienia oryginałów lub notarialnie potwierdzonych kopii dokumentów (jeśli przedstawione kserokopie będą nieczytelne lub będą wzbudzać wątpliwości co do ich prawdziwości).
10. **Informacja o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń i dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami.**
	1. Oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują pisemnie, drogą elektroniczną lub faksem.
	2. Jeżeli Zamawiający lub Wykonawca przekazują oświadczenia, wnioski, zawiadomienia oraz informacje za pośrednictwem faksu lub drogą elektroniczną, każda ze stron
	na żądanie drugiej niezwłocznie potwierdza fakt ich otrzymania.
	3. Wykonawca w odpowiedzi na otrzymane wezwanie, przekazuje dokumenty, wyjaśnienia lub oświadczenia w formie pisemnej tj. w oryginale lub kopii potwierdzonej za zgodność
	z oryginałem przez osobę uprawnioną do składania oświadczeń woli, bezwzględnie
	w terminie wyznaczonym w piśmie na adres Zamawiającego.
	4. Adres i osoba do kontaktu w zakresie dotyczącym przedmiotu zamówienia oraz
	w zakresie ustawy Pzp – Elżbieta Kostrzewa, ul. Kościelna 37, 60-537 Poznań;
	fax (61) 846-38-33, e-mail: zamowienia.publiczne@wup.poznan.pl
	5. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SIWZ.
	6. Zamawiający jest zobowiązany niezwłocznie udzielić wyjaśnień, jednak nie później niż
	na 2 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek
	o wyjaśnienie treści SIWZ, wpłynął do Zamawiającego nie później niż do końca dnia,
	w którym upływa połowa wyznaczonego terminu składania ofert.
	7. Zamawiający jednocześnie przekazuje treść wyjaśnienia wszystkim Wykonawcom, którym przekazano SIWZ, bez ujawniania źródła zapytania, a jeżeli specyfikacja jest udostępniona na stronie Internetowej, zamieszcza na tej stronie.
	8. Zamawiający nie zamierza zwoływać zebrania Wykonawców w celu wyjaśnienia wątpliwości, które dotyczą treści SIWZ.
	9. W uzasadnionych przypadkach, Zamawiający może przed upływem terminu składania ofert zmienić treść SIWZ, zgodnie z art. 38 ust. 4 ustawy Pzp.
	10. Zamawiający może przedłużyć termin składania ofert, z uwzględnieniem czasu niezbędnego do wprowadzenia w ofertach zmian, wynikających ze zmiany treści SIWZ, zgodnie z art. 38 ust. 6 ustawy Pzp.
	11. Niniejsze postępowanie prowadzi się w języku polskim, w związku z tym wszelkie pisma, wnioski, zawiadomienia, informacje, prośby, dokumenty, oświadczenia, itp. składane w trakcie postępowania między Zamawiającym a Wykonawcami muszą być sporządzone w języku polskim. Dokumenty sporządzone w języku obcym muszą być złożone
	z tłumaczeniem na język polski. Zamawiający prowadzi korespondencję z Wykonawcami wyłącznie w języku polskim.
11. **Wymagania dotyczące wadium.**

Zamawiający nie wymaga złożenia wadium.

**IX. Zastrzeżenie Wykonawcy o nie udostępnianie informacji zawartych w ofercie.**

* 1. Nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, nie później niż
	w terminie składania ofert, zastrzegł, że nie mogą być one udostępniane oraz wykazał,
	iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
	2. Uzasadnienie powinno w sposób możliwie najbardziej wyczerpujący potwierdzać,
	że okoliczności uzasadniające uznanie informacji za tajemnicę przedsiębiorstwa faktycznie zaistniały. Zastrzeżenie zakazu udostępniania informacji dokonane przez Wykonawcę staje się skuteczne dopiero w sytuacji, gdy Zamawiający w wyniku dokonania oceny zasadności i prawidłowości ich zastrzeżenia, uzna, że informacje
	te mają charakter tajemnicy przedsiębiorstwa w rozumieniu przepisów ustawy
	o zwalczaniu nieuczciwej konkurencji.
	3. Zawarte w ofercie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji należy oznaczyć klauzulą: Nie udostępniać - informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.) i załączyć do oferty jako odrębną część, nie złączoną z ofertą w sposób trwały.
	4. Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust. 4 ustawy Pzp. W sytuacji, gdy Wykonawca zastrzeże w ofercie informacje, które nie stanowią tajemnicy przedsiębiorstwa, albo są jawne na podstawie przepisów ustawy Pzp lub odrębnych przepisów, informacje te będą podlegały udostępnieniu na takich samych zasadach,
	jak pozostałe niezastrzeżone dokumenty.
1. **Termin związania ofertą.**
	1. Termin związania ofertą wynosi 30 dni.
	2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
2. **Opis sposobu przygotowywania ofert.**
3. Oferta powinna być przygotowana zgodnie z wymaganiami SIWZ oraz ustawy Pzp, zawierać wszystkie wymagane dokumenty, oświadczenia i załączniki, o których mowa
w treści niniejszej SIWZ.
4. Wykonawca składa w szczególności:
	1. Wypełniony załącznik nr 2 do SIWZ – Formularz oferty,
	2. Wypełnione pozycje w kolumnie nr 3 w tabelach A i B w załączniku nr 1 do SIWZ – dot. **części 1**,
	3. Dokumenty i oświadczenia z rozdziału VI SIWZ,
	4. Oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych - dot. **części 2**.
5. Każdy Wykonawca może złożyć tylko jedną ofertę w danej części, w której musi być zaoferowana tylko jedna cena. Złożenie większej liczby ofert w danej części spowoduje odrzucenie wszystkich ofert złożonych przez danego Wykonawcę
6. W ofercie Wykonawca winien skalkulować cenę dla całości przedmiotu zamówienia
w danej części.
7. Istnieje możliwość składania jednej oferty przez dwóch lub więcej Wykonawców
(w ramach oferty wspólnej) w rozumieniu art. 23 ustawy Pzp, pod warunkiem, że taka oferta spełniać będzie następujące wymagania:
	1. Zamawiający wymaga wskazania podmiotów składających ofertę wspólną (pełną nazwę i adres siedziby).
	2. Wykonawcy są zobowiązani ustanowić pełnomocnika do reprezentowania ich
	w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu
	i zawarcia umowy w sprawie zamówienia publicznego. Umocowanie pełnomocnika może wynikać z treści umowy lub zostać przedłożone oddzielnie wraz z ofertą.
8. Załączniki dołączone do SIWZ przedstawiane są w formie wzorów. Wykonawca może przedstawić załączniki wg własnego układu graficznego, lecz muszą one zawierać wszystkie zapisy i informacje ujęte we wzorach.
9. Oferta powinna być sporządzona w języku polskim oraz napisana pismem maszynowym, komputerowym albo czytelnym pismem odręcznym.
10. Oferta oraz wszystkie załączniki wymagają podpisu osób uprawnionych
do reprezentowania i składania oświadczenia woli w imieniu Wykonawcy, zgodnie
z odpowiednim wpisem do właściwego rejestru lub ewidencji, wymaganiami ustawowymi oraz przepisami prawa, a strony dokumentów oferty, które nie wymagają podpisu winny być parafowane przez te osoby.
11. W przypadku, gdy osoba podpisująca ofertę w imieniu Wykonawcy nie jest wpisana
do właściwego rejestru lub ewidencji jako osoba upoważniona do reprezentowania
i składania oświadczenia woli w imieniu Wykonawcy, musi do oferty dołączyć pełnomocnictwo w formie oryginału lub kopii poświadczonej notarialnie.
12. Za pożądane Zamawiający uważa zszycie/spięcie stron oferty w sposób zapobiegający zdekompletowaniu zawartości oraz ponumerowanie stron, a także sporządzenie przez Wykonawcę i dołączenie spisu treści.
13. Każda zmiana i poprawka w ofercie winna być naniesiona czytelnie i parafowana przez osobę upoważnioną do podpisywania oferty.
14. Wszelkie koszty związane z przygotowaniem i złożeniem oferty ponosi Wykonawca.
15. **Miejsce oraz termin składania i otwarcia ofert.**
16. Oferty należy składać w Wojewódzkim Urzędzie Pracy w Poznaniu, ul. Kościelna 37,
60-537 Poznań w terminie do dnia 15.10.2015 r. do godziny 10:30.
17. Oferty otrzymane po terminie składania ofert, zostaną niezwłocznie zwrócone Wykonawcom.
18. Ofertę należy umieścić w zamkniętym opakowaniu, uniemożliwiającym odczytanie zawartości, bez uszkodzenia tego opakowania. Opakowanie winno być oznaczone nazwą i adresem Wykonawcy oraz zaadresowane i opisane następująco:

|  |
| --- |
| ***Nazwa (firma) Wykonawcy******adres Wykonawcy*****Wojewódzki Urząd Pracy w Poznaniu****ul. Kościelna 37****60-537 Poznań****Przetarg nieograniczony:****Dostawa sprzętu komputerowego i oprogramowania dla Wojewódzkiego Urzędu Pracy w Poznaniu w 2015 r.****Nie otwierać przed dniem 15.10.2015 r. godz. 11:00** |

1. Wykonawca może, przed upływem terminu składania ofert, zmienić lub wycofać ofertę.
2. Wycofanie oferty następuje poprzez złożenie przez Wykonawcę pisemnego oświadczenia, że ofertę wycofuje. Oświadczenie o wycofaniu oferty musi zawierać
co najmniej nazwę i adres Wykonawcy, treść oświadczenia o wycofaniu oferty oraz podpis Wykonawcy. Dla identyfikacji składającego oświadczenie o wycofaniu oferty Zamawiającemu należy przedłożyć wypis z właściwego rejestru.
3. Zmiana oferty może być dokonana w dwojaki sposób: albo przez wycofanie złożonej oferty i złożenie nowej, albo przez złożenie odrębnego oświadczenia określającego zakres tych zmian. Powyższe oświadczenie powinno być złożone w taki sposób jak oferta, z dopiskiem „zmiana oferty”. Oświadczenie o zmianie oferty musi zawierać

co najmniej nazwę i adres Wykonawcy, treść oświadczenia oraz podpis Wykonawcy.

1. Otwarcie ofert jest jawne i nastąpi w dniu 15.10.2015 r. o godzinie 11:00w Wojewódzkim Urzędzie Pracy w Poznaniu, ul. Kościelna 37, 60-537 Poznań, II p., pokój nr 33.
2. Bezpośrednio przed otwarciem ofert, Zamawiający podaje kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
3. Podczas otwarcia ofert Zamawiający podaje nazwy (firmy) oraz adresy Wykonawców,
a także informacje dotyczące ceny, terminu wykonania zamówienia i warunków płatności zawartych w ofertach.
4. Informacje, o których mowa w niniejszym rozdziale pkt 8 i 9, Zamawiający przekazuje niezwłocznie Wykonawcom, którzy nie byli obecni przy otwarciu ofert, na ich wniosek.
5. W toku badania i oceny ofert, Zamawiający może żądać od Wykonawców wyjaśnień, dotyczących treści złożonych ofert.
6. Zamawiający poprawia w ofercie oczywiste omyłki pisarskie, oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek oraz inne omyłki, zgodnie z zapisami art. 87 ust. 2 ustawy Pzp, niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.
7. Zamawiający wyklucza Wykonawcę z postępowania o udzielenie zamówienia, zgodnie
z art. 24 ustawy Pzp.
8. Zamawiający odrzuca ofertę, jeżeli zaistnieje którakolwiek z przesłanek przewidzianych
w art. 89 ustawy Pzp.
9. Zamawiający unieważnia postępowanie o udzielenie zamówienia, zgodnie
z art. 93 ustawy Pzp.
10. **Opis sposobu obliczenia ceny.**
	* 1. Wykonawca uwzględniając wszystkie wymogi, o których mowa w SIWZ, powinien
		w cenie brutto ująć wszelkie koszty niezbędne dla prawidłowego i pełnego wykonania przedmiotu zamówienia oraz inne opłaty i podatki oraz ewentualne upusty
		i rabaty zastosowane przez Wykonawcę.

CENA BRUTTO = CENA NETTO + NALEŻNY PODATEK

* + 1. Cena brutto winna być wyrażona w złotych polskich, w złotych polskich będą prowadzone również rozliczenia pomiędzy Zamawiającym a Wykonawcą. Całkowita cena brutto wykonania zamówienia powinna być wyrażona liczbowo i słownie oraz podana z dokładnością do dwóch miejsc po przecinku.
		2. Ceny określone przez Wykonawcę w ofercie nie będą zmieniane w toku realizacji przedmiotu zamówienia.
		3. Nie przewiduje się żadnych przedpłat ani zaliczek na poczet realizacji przedmiotu umowy, a płatność nastąpi zgodnie z zapisami w umowie.
		4. Stawka VAT musi być określona zgodnie z ustawą z 11 marca 2004 r. o podatku
		od towarów i usług (t. j. Dz. U. z 2011, Nr 177, poz. 1054 ze zmianami).
1. **Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty wraz z podaniem znaczenia tych kryteriów i sposobu oceny ofert.**

**Część 1**

1. Oceniane kryteria i ich ranga:
2. cena brutto 94%
3. długość okresu gwarancji dla zestawów komputerowych 6%

Zamawiający przyjmuje, że 1% odpowiada 1 pkt.

Maksymalna liczba punktów w kryterium równa jest określonej wadze kryterium w %.

1. Kryterium określone w ust. 1 pkt a (P1) oceniane będzie według poniższego wzoru:

 Cena najniższa

 P1=------------------------------ x 94 pkt

 Cena badanej oferty

1. Kryterium określone w ust. 1 pkt b (P2) oceniane będzie w następujący sposób:
2. 48 miesięczny okres gwarancji 3 pkt,
3. 60 miesięczny okres gwarancji 6 pkt

**W przypadku, gdy Wykonawca w ust. 1 załącznika nr 2 do SIWZ - Formularz oferty,
nie wskaże długości okresu gwarancji lub wskaże maksymalny minimalny
tj. 36 miesięcy, Wykonawca otrzyma 0 punktów w tym kryterium. Wskazanie okresu gwarancji niższego od wymaganego spowoduje odrzucenie oferty jako niezgodnej
z SIWZ.**

**Część 2**

1. Oceniane kryteria i ich ranga:
2. cena brutto 90%
3. termin dostawy 10%

Zamawiający przyjmuje, że 1% odpowiada 1 pkt.

Maksymalna liczba punktów w kryterium równa jest określonej wadze kryterium w %.

1. Kryterium określone w ust. 1 pkt a (P1) oceniane będzie według poniższego wzoru:

 Cena najniższa

 P1=------------------------------ x 90 pkt

 Cena badanej oferty

1. Kryterium określone w ust. 1 pkt b (P2) oceniane będzie według poniższego wzoru:

Najkrótszy termin dostawy

P2 = -------------------------------------------- x 10 pkt

Termin dostawy badanej oferty

Termin dostawy zamówienia liczony będzie w dniach kalendarzowych. Maksymalny termin dostawy to 21 dni kalendarzowych.

**W przypadku, gdy Wykonawca w ust. 1 załącznika nr 2 do SIWZ - Formularz oferty, nie wskaże terminu dostawy lub wskaże maksymalny termin dostawy (tj. 21 dni kalendarzowych), Wykonawca otrzyma 0 punktów w tym kryterium.**

1. Punkty wynikające z algorytmu matematycznego, uzyskane przez Wykonawcę zostaną zaokrąglone do dwóch miejsc po przecinku.
2. Za najkorzystniejszą uważa się ofertę, która otrzymała najwyższą liczbę punktów
w danej części, zgodnie ze wzorem:

 P = P1 + P2

1. Zamawiający udzieli zamówienia Wykonawcy, którego oferta:
2. odpowiada wymaganiom określonym w ustawie o zamówieniach publicznych,
3. odpowiada wszystkim wymaganiom stawianym w SIWZ,
4. została uznana przez Zamawiającego za najkorzystniejszą w danej części.
5. **Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego.**
6. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający zawiadamia Wykonawców, którzy złożyli oferty, o:
7. wyborze najkorzystniejszej oferty, podając nazwę (firmę) albo imię i nazwisko, siedzibę albo miejsce zamieszkania i adres Wykonawcy, którego ofertę wybrano, uzasadnienie jej wyboru oraz nazwy (firmy) albo imiona i nazwiska, siedziby albo miejsca zamieszkania i adresy Wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację;
8. Wykonawcach, których oferty zostały odrzucone, podając uzasadnienie faktyczne
i prawne;
9. Wykonawcach, którzy zostali wykluczeni z postępowania o udzielenie zamówienia, podając uzasadnienie faktyczne i prawne;
10. terminie, określonym zgodnie z art. 94 ust. 1 lub 2 ustawy Pzp, po którego upływie umowa w sprawie zamówienia publicznego może być zawarta.
11. Informacje, o których mowa w ust. 1 pkt 1.1. niniejszego rozdziału, Zamawiający zamieszcza również na własnej stronie Internetowej oraz w swojej siedzibie na „tablicy ogłoszeń”.
12. Zamawiający zawiera umowę w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane w sposób określony w art. 27 ust. 2 ustawy Pzp, albo 10 dni – jeżeli zostało przesłane w inny sposób. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem tego terminu, jeżeli:
	1. w postępowaniu o udzielenie zamówienia została złożona tylko jedna oferta;
	2. w postępowaniu o udzielenie zamówienia nie odrzucono żadnej oferty oraz
	nie wykluczono żadnego Wykonawcy.
13. Jeżeli Wykonawca, którego oferta została wybrana uchyla się od zawarcia umowy
w sprawie zamówienia publicznego, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzania ich ponownego badania i oceny, chyba,
że zachodzą przesłanki unieważnienia postępowania, o których mowa w art. 93 ust. 1 ustawy Pzp.
14. W przypadku oferty wspólnej – przed podpisaniem umowy należy przedłożyć oryginał lub poświadczoną za zgodność z oryginałem kopię umowy regulującej współpracę Wykonawców, którzy złożyli ofertę wspólną, jeżeli nie została złożona wcześniej.
15. Niezwłocznie po zawarciu umowy w sprawie zamówienia publicznego Zamawiający zamieści ogłoszenie o udzieleniu zamówienia w Biuletynie Zamówień Publicznych.
16. **Wymagania dotyczące zabezpieczenia należytego wykonania umowy.**

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

1. **Istotne postanowienia umowy.**

**Część 1:**

**§ 1**

1. Przedmiotem umowy jest dostawa nw. sprzętu komputerowego i oprogramowania:
2. zestawy komputerowe wraz z oprogramowaniem – 16 szt.,
3. aktualizacja i rozszerzenie oprogramowania antywirusowego na stacje robocze
i serwery wraz z konsolą do centralnej administracji:
4. aktualizacje - 310 szt.,
5. nowe licencje – 7 szt.
6. program do zdalnej kontroli i zdalnego współdzielenia pulpitu przez internet – 1 szt.

zgodnie z ofertą Wykonawcy z dnia …………………, stanowiącą integralną część niniejszej umowy.

1. Wykonawca oświadcza, że przedmiot umowy:
	* 1. odpowiada ściśle wymogom określonym w SIWZ i w ofercie Wykonawcy,
		2. spełnia obowiązujące normy i parametry dopuszczające je do sprzedaży oraz używania na terenie Polski oraz krajów UE,
		3. posiada znak zgodności CE.
2. Przedmiot umowy, o którym mowa w ust. 1 pkt 1, jest fabrycznie nowy, nieużywany
i gotowy do pracy bez żadnych dodatkowych zakupów czy inwestycji.

**§ 2**

1. Wykonawca dostarczy przedmiot umowy, określony w § 1 ust. 1 umowy,
na własne ryzyko (wraz z załadunkiem i rozładunkiem), w ramach wynagrodzenia określonego w § 4 ust. 1 umowy, do siedziby Zamawiającego – Poznań, ul. Kościelna 37,
od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy, w godzinach pracy Urzędu, w terminie do 21 dni kalendarzowych od daty podpisania umowy.
2. Dostarczony sprzęt komputerowy musi być tak zapakowany, aby zapobiec jego uszkodzeniu lub pogorszeniu stanu podczas transportu do miejsca przeznaczenia.
3. Wykonawca jest zobowiązany zawiadomić Zamawiającego o planowanym terminie dostawy sprzętu komputerowego z co najmniej 1-dniowym wyprzedzeniem.
4. Wykonawca zobowiązany jest wraz z dostawą sprzętu komputerowego
i oprogramowania dołączyć instrukcje obsługi i eksploatacji w języku polskim.
5. Licencja na oprogramowanie, o którym mowa w § 1 ust. 1 pkt 2 i 3, zostaje udzielona
na okres:
	* + 1. na oprogramowanie antywirusowe – od 19.11.2015 r. do 18.11.2016 r.,
			2. na program do zdalnej kontroli i zdalnego współdzielenia pulpitu przez internet
			– od 22.11.2015 r. do 21.11.2016 r.
6. Wykonawca gwarantuje Zamawiającemu, że udzielając licencji na korzystanie
z oprogramowania, nie narusza żadnych praw osób trzecich oraz nie zachodzą jakiekolwiek podstawy do zgłoszenia przez osoby trzecie roszczeń do tych praw.
7. Wszelkie opłaty i wynagrodzenia autorskie za licencję, zawarte są w cenie przedmiotu umowy, o którym mowa w § 4 ust.1 umowy.

**§ 3**

Strony postanawiają, że warunkiem odbioru będzie podpisany przez obie Strony protokół odbioru przedmiotu umowy (z numerami seryjnymi urządzeń, numerami licencji oprogramowania), którego data oznacza termin rozpoczęcia gwarancji oraz wystawienia faktury.

**§ 4**

1. Wykonawcy za wykonanie przedmiotu niniejszej umowy w całości przysługuje wynagrodzenie w wysokości ……………… zł brutto (słownie: ………………….złotych).
2. Wynagrodzenie określone w ust. 1 obejmuje wszystkie koszty związane z wykonaniem umowy.
3. Niedoszacowanie, pominięcie lub nieprawidłowy sposób skalkulowania wysokości kosztów związanych z realizacją przedmiotu umowy, nie może być podstawą
do żądania zmiany wynagrodzenia określonego w ust. 1, nawet, gdy koszty te wzrosną
w trakcie jej realizacji, poza przypadkiem zmian w obowiązujących przepisach podatkowych.
4. Podstawą wystawienia faktury jest podpisanie protokołu odbioru przedmiotu umowy,
o którym mowa w § 3 umowy.
5. Zamawiający dokona zapłaty wynagrodzenia w terminie 21 dni od daty doręczenia prawidłowo wystawionej faktury przez Wykonawcę.
6. Wynagrodzenie przysługujące Wykonawcy jest płatne przelewem ze środków Funduszu Pracy, na konto Wykonawcy nr…………………………………
7. Zamawiający wyraża zgodę na wystawienie i otrzymanie faktury w dowolnym formacie elektronicznym[[1]](#footnote-1).
8. Faktura VAT w formie elektronicznej zostanie przesłana z adresu e-mail Wykonawcy: …………………… na adresy e-mail Zamawiającego: ……………………[[2]](#footnote-2).
9. Za datę płatności ustala się dzień obciążenia rachunku Zamawiającego.

**§ 5**

1. Wykonawca na dostarczony przedmiot umowy, o którym mowa w § 1 ust. 1 pkt 1 umowy, udziela gwarancji na okres ………. miesięcy[[3]](#footnote-3) liczony od daty podpisania protokołu zdawczo-odbiorczego, o którym mowa w § 3 umowy.
2. Wykonawca, w ramach wynagrodzenia określonego w § 4 ust. 1, zobowiązany jest
do wykonywania napraw w okresie gwarancji.
3. Serwis przedmiotu umowy, o którym mowa w § 1 ust. 1 pkt 1 umowy, musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta.
4. W przypadku awarii urządzeń w okresie wskazanym w ust. 1 Wykonawca przystąpi
do ich naprawy w terminie nie przekraczającym 24 godziny od zgłoszenia awarii (w dni robocze, pon.-pt, z wyłączeniem dni ustawowo wolnych od pracy).
5. Czas usunięcia awarii musi być nie dłuższy niż 48 godzin od jej zgłoszenia. W sytuacji, gdy usterka dotyczy podzespołu, który trzeba sprowadzić od producenta czas naprawy urządzenia nie może przekroczyć 14 dni kalendarzowych, o czym Wykonawca jest zobowiązany poinformować Zamawiającego nie później niż w terminie 48 godzin
od zgłoszenia awarii.
6. Jeżeli naprawa będzie trwała dłużej niż 48 godzin, Wykonawca zobowiązany jest
do dostarczenia urządzenia zastępczego o porównywalnych parametrach, do czasu naprawy urządzenia uszkodzonego.
7. Serwis gwarancyjny świadczony będzie w miejscu użytkowania urządzeń i w godzinach urzędowania Zamawiającego, tj. w godz. 7.30 – 15.30. W sytuacji wystąpienia konieczności naprawy poza siedzibą Zamawiającego, Wykonawca zobowiązany jest:
	1. odebrać uszkodzone urządzenia, najpóźniej w dniu następnym po stwierdzeniu konieczności naprawy poza siedzibą Zamawiającego,
	2. dostarczyć naprawione urządzenia do siedziby Zamawiającego,
	3. czynności określone w pkt a) i b) Wykonawca wykonuje na własny koszt i własnym transportem.
8. Każda naprawa gwarancyjna powoduje przedłużenie okresu gwarancji o czas trwania naprawy.
9. Wykonawca zobowiązuje się do wymiany urządzeń na nowe w okresie gwarancji
w przypadku wystąpienia dwóch istotnych awarii, których usunięcie związane będzie
z wymianą części lub podzespołów – przy drugiej awarii lub jeśli usunięcie awarii jest niemożliwe. Wymiana powinna nastąpić w ciągu 14 dni od daty zgłoszenia przez Zamawiającego. Na ten czas Wykonawca zobowiązany jest dostarczyć urządzenia zastępcze o parametrach nie gorszych niż wymieniane.
10. W przypadku wymiany uszkodzonego urządzenia na nowe lub wymiany jego części lub podzespołów w związku z okolicznościami określonymi w ust. 8, w stosunku do nowego, wymienionego urządzenia obowiązują warunki gwarancji i serwisu wynikające ze złożonej oferty.
11. Uprawnienia Zamawiającego z tytułu gwarancji nie wyłączają odpowiedzialności Wykonawcy z tytułu rękojmi.
12. Jeżeli z jakiegokolwiek powodu leżącego po stronie Wykonawcy, nie usunie on wady (usterki) w wyznaczonym terminie, Zamawiający ma prawo w trybie pozasądowym zaangażować innego Wykonawcę do usunięcia wad (usterek), a Wykonawca zobowiązany jest pokryć związane z tym koszty, w ciągu 14 dni od daty otrzymania dowodu zapłaty, na co Wykonawca wyraża zgodę.
13. Warunki gwarancji nie mogą nakazywać Zamawiającemu przechowywania opakowań
w których urządzenia zostaną dostarczone (zamawiający może usunąć opakowania urządzeń po ich dostarczeniu, co nie spowoduje utraty gwarancji, a dostarczony sprzęt mimo braku opakowań będzie podlegał usłudze gwarancyjnej).

**§ 6**

1. Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% wartości umowy określonej w § 4 ust. 1, w razie wypowiedzenia umowy przez którąkolwiek za Stron
z przyczyn leżących po stronie Wykonawcy.
2. W przypadku opóźnienia w dostawie przedmiotu umowy, o którym mowa
w § 2 ust. 1 umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 0,1% wynagrodzenia określonego w § 4 ust. 1 umowy - za każdy dzień opóźnienia.
3. Wykonawca zobowiązany jest do zapłaty kary umownej w terminie 7 dni od daty wezwania do jej zapłacenia.
4. Jeżeli kara umowna nie pokrywa poniesionej szkody, Strony mogą dochodzić odszkodowania uzupełniającego na zasadach ogólnych.

§ 7

Do współpracy w sprawach związanych z wykonaniem umowy wyznacza się:

* 1. ze strony Zamawiającego: …………………., tel. …………., e-mail: ……………
	2. ze strony Wykonawcy: …………………., tel. ………………, e-mail: ……………

§ 8

1. Do niniejszej umowy mają zastosowanie przepisy ustawy Prawo zamówień publicznych, a w sprawach w niej nieuregulowanych stosuje się przepisy Kodeksu Cywilnego.
2. Zmiany umowy wymagają dla swej ważności formy pisemnej pod rygorem nieważności.

**§ 9**

Sądem właściwym dla wszystkich spraw, które wynikną z realizacji tej umowy będzie sąd powszechny w Poznaniu.

**Część 2:**

**§ 1**

1. Przedmiotem umowy jest:
	* 1. Zakup i wdrożenie Forti Analyzer 200D, zwanego dalej urządzeniem.
		2. Odnowienie licencji i przedłużenie usług Vmware.

 zgodnie z ofertą Wykonawcy z dnia …………………, stanowiącą integralną część niniejszej umowy.

1. Wykonawca oświadcza, że przedmiot umowy:
	* 1. odpowiada ściśle wymogom określonym w SIWZ i w ofercie Wykonawcy,
		2. spełnia obowiązujące normy i parametry dopuszczające je do sprzedaży oraz używania na terenie Polski oraz krajów UE,
		3. posiada znak zgodności CE.
2. Przedmiot umowy, o którym mowa w ust. 1 pkt 1, jest fabrycznie nowy, nieużywany
i gotowy do pracy bez żadnych dodatkowych zakupów czy inwestycji.
3. Serwis winien być realizowany przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu mających swoją siedzibę na terenie Polski. Zgłoszenia serwisowe przyjmowane w trybie 8x5 przez dedykowany serwisowy moduł internetowy ………………….(należy podać adres www) oraz infolinię 24x7 ………………..(należy podać numer infolinii).
4. Wykonawca przeprowadzi szkolenie dla administratorów Zamawiającego, w siedzibie Zamawiającego w zakresie bieżącej obsługi i eksploatacji urządzenia, w terminie
do 14 dni kalendarzowych od daty dostawy.

**§ 2**

1. Wykonawca dostarczy przedmiot umowy, określony w § 1 ust. 1 umowy,
na własne ryzyko (wraz z załadunkiem i rozładunkiem), w ramach wynagrodzenia określonego w § 4 ust. 1 umowy, do siedziby Zamawiającego – Poznań, ul. Kościelna 37,
od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy, w godzinach pracy Urzędu, w terminie ……… dni kalendarzowych[[4]](#footnote-4) od daty podpisania umowy.
2. Dostarczone urządzenie musi być tak zapakowane, aby zapobiec jego uszkodzeniu lub pogorszeniu stanu podczas transportu do miejsca przeznaczenia.
3. Wykonawca jest zobowiązany zawiadomić Zamawiającego o planowanym terminie dostawy urządzenia z co najmniej 1-dniowym wyprzedzeniem.
4. Wykonawca zobowiązany jest wraz z dostawą urządzenia i oprogramowania dołączyć instrukcje obsługi i eksploatacji w języku polskim.
5. Licencja na oprogramowanie, o którym mowa w § 1 ust. 1 pkt 2, zostaje udzielona
na okres od daty podpisania umowy do 13.10.2018 r.
6. Wykonawca gwarantuje Zamawiającemu, że udzielając licencji na korzystanie
z oprogramowania, nie narusza żadnych praw osób trzecich oraz nie zachodzą jakiekolwiek podstawy do zgłoszenia przez osoby trzecie roszczeń do tych praw.
7. Wszelkie opłaty i wynagrodzenia autorskie za licencję, zawarte są w cenie przedmiotu umowy, o którym mowa w § 4 ust.1 umowy.

**§ 3**

Strony postanawiają, że warunkiem odbioru będzie podpisany przez obie Strony protokół odbioru przedmiotu umowy (z numerami seryjnymi urządzenia, numerami licencji oprogramowania), którego data oznacza termin rozpoczęcia gwarancji oraz wystawienia faktury.

**§ 4**

1. Wykonawcy za wykonanie przedmiotu niniejszej umowy w całości przysługuje wynagrodzenie w wysokości ……………… zł brutto (słownie: ………………….złotych).
2. Wynagrodzenie określone w ust. 1 obejmuje wszystkie koszty związane z wykonaniem umowy.
3. Niedoszacowanie, pominięcie lub nieprawidłowy sposób skalkulowania wysokości kosztów związanych z realizacją przedmiotu umowy, nie może być podstawą
do żądania zmiany wynagrodzenia określonego w ust. 1, nawet, gdy koszty te wzrosną
w trakcie jej realizacji, poza przypadkiem zmian w obowiązujących przepisach podatkowych.
4. Podstawą wystawienia faktury jest podpisanie protokołu odbioru przedmiotu umowy,
o którym mowa w § 3 umowy.
5. Zamawiający dokona zapłaty wynagrodzenia w terminie 21 dni od daty doręczenia prawidłowo wystawionej faktury przez Wykonawcę.
6. Wynagrodzenie przysługujące Wykonawcy jest płatne przelewem ze środków Funduszu Pracy, na konto Wykonawcy nr…………………………………
7. Zamawiający wyraża zgodę na wystawienie i otrzymanie faktury w dowolnym formacie elektronicznym[[5]](#footnote-5).
8. Faktura VAT w formie elektronicznej zostanie przesłana z adresu e-mail Wykonawcy: …………………… na adresy e-mail Zamawiającego: ……………………[[6]](#footnote-6).
9. Za datę płatności ustala się dzień obciążenia rachunku Zamawiającego.

**§ 5**

1. Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% wartości umowy określonej w § 4 ust. 1, w razie wypowiedzenia umowy przez którąkolwiek za Stron
z przyczyn leżących po stronie Wykonawcy.
2. W przypadku opóźnienia w dostawie przedmiotu umowy, o którym mowa
w § 2 ust. 1 umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 0,1% wynagrodzenia określonego w § 4 ust. 1 umowy - za każdy dzień opóźnienia.
3. Wykonawca zobowiązany jest do zapłaty kary umownej w terminie 7 dni od daty wezwania do jej zapłacenia.
4. Jeżeli kara umowna nie pokrywa poniesionej szkody, Strony mogą dochodzić odszkodowania uzupełniającego na zasadach ogólnych.

§ 6

Do współpracy w sprawach związanych z wykonaniem umowy wyznacza się:

* 1. ze strony Zamawiającego: …………………., tel. …………., e-mail: ……..……..
	2. ze strony Wykonawcy: …………………., tel. ………………, e-mail: ……………

§ 7

1. Do niniejszej umowy mają zastosowanie przepisy ustawy Prawo zamówień publicznych, a w sprawach w niej nieuregulowanych stosuje się przepisy Kodeksu Cywilnego.
2. Zmiany umowy wymagają dla swej ważności formy pisemnej pod rygorem nieważności.

**§ 8**

Sądem właściwym dla wszystkich spraw, które wynikną z realizacji tej umowy będzie sąd powszechny w Poznaniu.

1. **Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy
 w toku postępowania o udzielenie zamówienia.**

Zamawiający informuje, iż szczegółowe uregulowanie środków ochrony prawnej zawarte jest
w dziale VI ustawy, tj. art. 179 – 198 g Pzp.

1. **Pozostałe informacje.**
	* + - 1. Zamawiający dopuszcza składanie ofert częściowych.
				2. Zamawiający nie przewiduje zawarcia umowy ramowej.
				3. Zamawiający nie przewiduje udzielania zamówień uzupełniających, o których mowa
				w art. 67 ust. 1 pkt 6 Pzp.
				4. Zamawiający nie dopuszcza składania ofert wariantowych.
				5. Adres poczty elektronicznej lub strony internetowej Zamawiającego z uwagi na fakt,
				iż dopuszcza się możliwość porozumiewania się drogą elektroniczną.

|  |  |
| --- | --- |
| **e-mail:** **zamowienia.publiczne@wup.poznan.pl** | **strona internetowa:** [**wuppoznan.praca.gov.pl**](http://www.wup.poznan.pl) |

* + - * 1. Informacje dotyczące walut obcych, w jakich mogą być prowadzone rozliczenia między Zamawiającym a Wykonawcą.

Rozliczenia pomiędzy Wykonawcą a Zamawiającym będą dokonywane w złotych polskich.

* + - * 1. Zamawiający nie przewiduje aukcji elektronicznej.
				2. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
				3. Zamawiający nie zamierza ustanawiać dynamicznego systemu zakupów.
				4. Załączniki stanowiące integralną część SIWZ:
* Załącznik nr 1 – Opis przedmiotu zamówienia,
* Załącznik nr 2 – Formularz oferty,
* Załącznik nr 3 – Oświadczenie o spełnieniu warunków udziału w postępowaniu,
* Załącznik nr 4 - Oświadczenie Wykonawcy o braku podstaw do wykluczenia,
* Załącznik nr 5 - Informacja Wykonawcy dot. przynależności do grupy kapitałowej,
* Załącznik nr 6 – Wykaz dostaw,
* Załącznik nr 7 – Wykaz osób – część 2.

Zatwierdzam

 Sławomir Wąsiewski

 Wicedyrektor
 Wojewódzkiego Urzędu Pracy w Poznaniu

Poznań, dnia 07.10.2015 r.

**Załącznik nr 1 do SIWZ**

**Opis przedmiotu zamówienia**

**CZĘŚĆ 1.**

Zamawiający dokonał opisu przedmiotu zamówienia poprzez wskazanie parametrów technicznych w kolumnie nr 2 poniższej tabeli. Zamawiający wymaga, aby przystępując do postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na: „Dostawę sprzętu komputerowego i oprogramowania dla Wojewódzkiego Urzędu Pracy w Poznaniu w 2014 r.”, Wykonawca złożył niniejszy załącznik z wypełnioną i podpisaną kolumną nr 3.

**Zestaw komputerowy – szt. 16**

|  |
| --- |
| Oferowane produkty muszą spełniać wszystkie parametry określone w niniejszym załączniku oraz oznakowane symbolem CE, pochodzić z legalnego źródła. * + - 1. Wszystkie opisane parametry wymagane są wymaganiami minimalnymi. Zamawiający akceptuje rozwiązania o parametrach równoważnych lub lepszych, bez utraty funkcjonalności i wydajności.
1. Wszystkie oferowane produkty muszą być sprawne, fabrycznie nowe, nieużywane.
 |

**Tabela A**

|  |  |
| --- | --- |
| **1.** | **Monitor LCD 17’’** |
|  | **Opis parametrów technicznych****wymagania minimalne** | **Parametry i wartości oferowane** |
| **1** | **2** | **3** |
| 1.1 | Format ekranu monitora: standardowy 5:4 |  |
| 1.2 | Przekątna ekranu: 17 cali |  |
| 1.3 | Typ panela LCD: TFT TN |  |
| 1.4 | Zalecana rozdzielczość obrazu: 1280 x 1024 pikseli |  |
| 1.5 | Częst. odświeżania przy zalecanej rozdzielczości: 60 Hz |  |
| 1.6 | Czas reakcji matrycy: max 5 ms |  |
| 1.7 | Deklarowana jasność: co najmniej: 250 cd/m2 |  |
| 1.8 | Deklarowany kontrast: co najmniej: 1000:1 |  |
| 1.9 | Kąt widzenia poziomy: co najmniej 160 stopni |  |
| 1.10 | Kąt widzenia pionowy: co najmniej 160 stopni |  |
| 1.11 | Liczba wyświetlanych kolorów: co najmniej 16,7 mln |  |
| 1.12 | Certyfikaty:CE, EPA Energy Star, TCO 5.0 |  |
| 1.13 | Regulacja cyfrowa (OSD): Tak |  |
| 1.14 | Głośniki: Nie |  |
| 1.15 | Mikrofon: Nie |  |
| 1.16 | Typ sygnału wejściowego: RGB |  |
| 1.17 | Typ gniazda wejściowego (sygnałowego): 15-stykowe D-Sub |  |
| 1.18 | Wbudowany zasilacz: Tak |  |
| 1.19 | Pobór mocy (praca/spoczynek): max. 28/2 Wat |  |
| 1.20 | Waga: do 4 kg |  |

**Tabela B**

|  |  |
| --- | --- |
| **2.** | **Komputer PC** |
|  | **Opis parametrów technicznych****wymagania minimalne** | **Parametry i wartości oferowane** |
| 1 | **2** | **3** |
| 2.1 | Typ: stacjonarny |  |
| 2.2 | Procesor: Procesor wielordzeniowy klasy x86, przeznaczony do pracy w stacjach roboczych, owydajności w teście PassMark- PerformanceTest 64bit - CPU Mark - min. 4116 pkt.Zamawiający wymaga załączenia do oferty wydruku z wydajności procesora wg testuwydajności PassMark- PerformanceTest 8.0 64bit- CPU Mark lub określenia typu/modelu procesora. (Wydruk z wydajności procesora powinien być podpisany przez osobęupoważnioną do reprezentowania Wykonawcy). |  |
| 2.3 | Pamięć: nie mniej niż 4GB, gniazda na pamięć – min. 4 |  |
| 2.4 | Dysk twardy o pojemności min. 1 TB |  |
| 2.5 | Płyta główna: częstotliwość pracy magistrali FSB – zgodna z oferowanym modelem procesoraWyposażona w złącza: 2 gniazda PCIe x1 o pełnej wysokości1 gniazdo PCIe x4 o pełnej wysokości1 gniazdo PCIe x16 o pełnej wysokości |  |
| 2.6 | Zintegrowana karta graficzna: zintegrowane porty: DisplayPort, D-Sub 15-Pin (VGA) |  |
| 2.7 | Zintegrowana karta dźwiękowa: Tak |  |
| 2.8 | Interfejsy:* 1 gniazdo mikrofonowe
* 1 gniazdo słuchawkowe
* 4 porty USB 3.0
* 4 porty USB 2.0
* 2 porty PS/2 (klawiatura i mysz)
* 1 port VGA
* 1 port DVI-D
* 1 wejście sygnałowe audio
* 1 wyjście sygnałowe audio
* 1 port RJ-45
* 1 port szeregowy
 |  |
| 2.9 | Napęd optyczny: DVD-RW  |  |
| 2.10 | Zasilacz: aktywny stabilizator PFC, moc 300W, zgodny z normą ENERGY STAR® |  |
| 2.11 | Obudowa typu Micro Tower, umożliwiająca pracę w pionie, możliwość podłączenia urządzeń przez minimum 2 porty USB 3.0 do przedniego panelu obudowy |  |
| 2.12 | Waga: do 7 kg |  |
| 2.13 | System operacyjny: Microsoft Windows 8 Pro z możliwością downgrade’u do Microsoft Windows 7 Professional PL lub równoważne rozwiązanie[[7]](#footnote-7)oraz zestaw płyt umożliwiający przywrócenie systemu |  |
| 2.14 | Oprogramowanie Microsoft Office Home &Business 2013 PL OEM lub rozwiązanie równoważne[[8]](#footnote-8) |  |
| 2.15 | Dołączone wyposażenie: |
| Klawiatura: standard – USB, ciche klawisze |  |
| Mysz optyczna, rolka, standard – USB |  |
| 2.16 | Certyfikaty i standardy: |
| Deklaracja zgodności CE |
| Certyfikat jakości ISO 9001: 2000 producenta komputera. |
| ENERGY STAR® |
| Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera |
| 2.17. | Zarządzanie:Funkcjonalność odnośnie zarządzania i monitorowania komputera na poziomie sprzętowym działającą niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC. W tym minimum: |
| monitorowanie konfiguracji komponentów komputera – CPU, pamięć, HDD, wersje BIOS płyty głównej; |
| zdalną konfigurację ustawień BIOS; |
| zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego CD ROM z serwera zarządzającego |

**Aktualizacja i rozszerzenie oprogramowania antywirusowego na stacje robocze**

**i serwery wraz z konsolą do centralnej administracji – szt. 310 plus 7 nowych**

|  |
| --- |
| **Aktualizacja licencji programu antywirusowego – 310 szt.** tj. aktualizacja posiadanego przez zamawiającego oprogramowania ESET Endpoint Antivirus poprzez dostarczenie 310 licencji ww. oprogramowania lub oprogramowania równoważnego, uprawniających do pobierania w okresie jednego roku uaktualnień bazy danych wirusów programu użytkowanego przez zamawiającego (tzw. roczna subskrypcja aktualizacji bazy danych wirusów).**Nowe licencje programu antywirusowego dla serwerów plikowych – 7 szt.**tj. nowe licencje na oprogramowania ESET File Security for Windows Server lub równoważnego wraz z roczną subskrypcją aktualizacji bazy danych wirusów.Zaoferowane oprogramowanie musi współpracować z wykorzystywanym przez zamawiającego centralnym serwerem zarządzającym oprogramowaniem ESET (Remote Administrator Server). Roczna subskrypcja aktualizacji bazy danych wirusów dla ww. licencji ma obowiązywać przez rok od 19 listopada 2015 r.Zamawiający dopuszcza zastosowanie innego, równoważnego rozwiązania pod warunkiem, że spełnia ono minimalne parametry przedstawione w poniższej specyfikacji:**Stacje Windows (dotyczy również serwerów Windows)**1. Pełne wsparcie dla systemu Windows 2000/XP/Vista/Windows 7/ Windows 8.2. Wsparcie dla Windows Security Center (Windows XP SP2).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. Pomoc w programie (help) w języku polskim.**Ochrona antywirusowa i antyspyware**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. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
5. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików „na żądanie” lub według harmonogramu.
6. System musi 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.
7. 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.
8. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń).
13. Możliwość umieszczenia na liście wyłączenia ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
14. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
15. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
16. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min. lub do ponownego uruchomienia komputera.
17. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
18. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
19. 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.
20. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird do wersji 5.x i Windows Live Mail (funkcje programu muszą być dostępne bezpośrednio z menu programu pocztowego).
21. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird do wersji 5.x, Windows Live Mail.
22. 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).
23. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
24. Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.
25. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
26. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch musi być automatycznie blokowany, a użytkownikowi wyświetlane stosowne powiadomienie.
27. 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.
28. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
29. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
30. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
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. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
34. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
35. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
36. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
37. 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.
38. 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 heurystyką ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
39. 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 możliwość określenia czy próbki zagrożeń mają być wysyłane w pełni automatycznie, czy też po dodatkowym potwierdzeniu przez użytkownika.
40. Do czasu wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego używanego na komputerze użytkownika.
41. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
42. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
43. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
44. Interfejs programu ma oferować funkcję pracy w trybie bez grafiki, gdzie cały interfejs wyświetlany jest w formie formatek i tekstu.
45. Interfejs programu ma mieć możliwość automatycznego aktywowania trybu bez grafiki w momencie, gdy użytkownik przełączy system Windows w tryb wysokiego kontrastu.
46. Możliwość zabezpieczenia konfiguracji programu hasłem w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
47. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę nawet w sytuacji, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
48. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby deinstalacji musi być takie samo.
49. Program musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
50. Program musi mieć możliwość definiowania typu aktualizacji systemowych, o braku których będzie informował użytkownika, w tym przynajmniej: aktualizacji krytycznych, aktualizacji ważnych, aktualizacji zwykłych, aktualizacji o niskim priorytecie oraz możliwość dezaktywacji tego mechanizmu.
51. 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.
52. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB musi umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
53. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
54. Program musi umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji, w tym przynajmniej: pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
55. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
56. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostępu w trybie do odczytu, pełnego dostępu, braku dostępu do podłączanego urządzenia.
57. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
58. W momencie podłączenia zewnętrznego nośnika, aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
59. Użytkownik ma posiadać możliwość takiej konfiguracji aplikacji, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
60. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
61. Moduł HIPS musi posiadać możliwość pracy w jednym z czterech trybów:
62. tryb automatyczny z regułami, gdzie aplikacja automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika;
63. tryb interaktywny, w którym aplikacja pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie;
64. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika;
65. tryb uczenia się, w którym aplikacja uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu aplikacja musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
66. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
67. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
68. 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.
69. 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.
70. 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.
71. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
72. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
73. Aplikacja musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
74. Aplikacja musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http.
75. Aplikacja musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
76. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
77. Aplikacja musi być w pełni zgodna z technologią Network Access Protection (NAP).
78. Program ma być w pełni zgodny z technologią CISCO Network Access Control.
79. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
80. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.
81. Użytkownik ma mieć możliwość skonfigurowania programu tak, aby automatycznie aplikacja włączała powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym, po określonym przez użytkownika czasie.
82. 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.
83. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
84. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór następujących modułów do instalacji: ochrona antywirusowa i antyspywerowa, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, kopia dystrybucyjna, obsługa technologii Microsoft NAP.

**Ochrona serwera plików Windows**1. Wsparcie dla systemów: Microsoft Windows Server 2000, 2003, 2008, 2008 R2, 2012, SBS 2003, 2003 R2, 2008, 2011, 2012.
2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
4. Wbudowana technologia do ochrony przed rootkitami.
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. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. System antywirusowy musi posiadać możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
10. System antywirusowy musi posiadać możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
11. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.
12. Możliwość skanowania dysków sieciowych i dysków przenośnych.
13. Skanowanie plików spakowanych i skompresowanych.
14. Możliwość definiowania listy rozszerzeń plików, które mają być skanowane (z uwzględnieniem plików bez rozszerzeń).
15. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
16. System antywirusowy musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
17. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
18. Dodanie automatycznych wyłączeń nie może wymagać restartu serwera.
19. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
20. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
21. W przypadku restartu serwera – usunięte z listy wyłączeń elementy muszą być automatycznie uzupełnione.
22. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
23. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
24. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
25. 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 heurystyką ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
26. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych, tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
27. Aktualizacje modułów analizy heurystycznej.
28. 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 możliwość określenia czy próbki zagrożeń będą wysyłane w pełni automatycznie, czy też po dodatkowym potwierdzeniu przez użytkownika.
29. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
30. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
31. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
32. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
33. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.
34. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
35. Interfejs programu ma oferować funkcję pracy w trybie bez grafiki, gdzie cały interfejs wyświetlany jest w formie formatek i tekstu.
36. Interfejs programu ma mieć możliwość automatycznego aktywowania trybu bez grafiki w momencie, gdy użytkownik przełączy system Windows w tryb wysokiego kontrastu.
37. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
38. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę nawet w sytuacji, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
39. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby deinstalacji musi być takie samo.
40. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.
41. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
42. System antywirusowy 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. Program musi także posiadać opcję dezaktywacji tego mechanizmu.
43. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
44. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
45. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
46. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: stacji dyskietek, napędów CD/DVD oraz portów USB.
47. Funkcja blokowania portów USB ma umożliwiać administratorowi zdefiniowanie listy portów USB w komputerze, które nie będą blokowane (wyjątki).
48. System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, informacji o aktywnych procesach i połączeniach.
49. 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.
50. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
51. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
52. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
53. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
54. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).
55. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej, a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu.
56. System antywirusowy musi być wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
57. Praca programu musi być niezauważalna dla użytkownika.
58. Dziennik zdarzeń musi rejestrować informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
59. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

**Konsola zdalnej administracji*** 1. Centralna instalacja programów służących do ochrony stacji roboczych Windows.
	2. Centralne zarządzanie programami służącymi do ochrony stacji roboczych Windows/Linux/ MAC OS.
	3. Centralna instalacja oprogramowania na końcówkach (stacjach roboczych) z systemami operacyjnymi typu 2000/XP Professional/Vista/Windows7/Windows 8.
	4. Do instalacji centralnej i zarządzania centralnego nie może być wymagany dodatkowy agent. Na końcówkach zainstalowany powinien być sam program antywirusowy.
	5. Komunikacja miedzy serwerem a klientami musi być zabezpieczona hasłem.
	6. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, zaporą osobistą i kontrolą dostępu do stron internetowych, zainstalowanymi na stacjach roboczych w sieci.
	7. Kreator konfiguracji zapory osobistej stacji klienckich pracujących w sieci, umożliwiający podgląd i utworzenie globalnych reguł w oparciu o reguły odczytane ze wszystkich lub z wybranych komputerów lub ich grup.
	8. Możliwość uruchomienia centralnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej.
	9. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych).
	10. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy.
	11. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
	12. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.
	13. Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnych dla zarządzanych programów.
	14. Możliwość importowania konfiguracji programu z wybranej stacji roboczej, a następnie przesłanie (skopiowanie) jej na inną stację lub grupę stacji roboczych w sieci.
	15. Możliwość zmiany konfiguracji na stacjach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko wtedy, gdy ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne).
	16. Możliwość uruchomienia serwera centralnej administracji i konsoli zarządzającej na stacjach Microsoft Windows: 8, 7, Vista, XP, 2000 oraz Windows Server: 2012, 2008 R2, 2008, 2003, 2000.
	17. Możliwość rozdzielenia serwera centralnej administracji od konsoli zarządzającej w taki sposób, że serwer centralnej administracji będzie instalowany na jednym serwerze/stacji, a konsola zarządzająca na tym samym serwerze i na stacjach roboczych należących do administratorów.
	18. Możliwość wymuszenia konieczności uwierzytelniania stacji roboczych przed połączeniem się z serwerem zarządzającym. Uwierzytelnianie przy pomocy zdefiniowanego na serwerze hasła.
	19. Do instalacji serwera centralnej administracji nie powinno być wymagane zainstalowanie żadnych dodatkowych baz typu MSDE lub MS SQL. Serwer centralnej administracji musi mieć własną wbudowaną bazę w pełni kompatybilną z formatem bazy danych programu Microsoft Access.
	20. Serwer centralnej administracji ma oferować administratorowi możliwość współpracy przynajmniej z trzema zewnętrznymi motorami baz danych w tym minimum z: Microsoft SQL Server, MySQL Server oraz Oracle.
	21. Do instalacji serwera centralnej administracji nie powinno być wymagane zainstalowanie dodatkowych aplikacji takich jak Internet Information Service (IIS) czy Apache.
	22. Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) w formacie HTML lub CSV.
	23. Aplikacja musi posiadać funkcjonalność, która umożliwi przesłanie wygenerowanych raportów na wskazany adres email.
	24. Do wysłania raportów aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na stacji, gdzie jest uruchomiona usługa serwera.
	25. Możliwość tworzenia hierarchicznej struktury serwerów zarządzających i replikowania informacji pomiędzy nimi w taki sposób, aby nadrzędny serwer miał wgląd w swoje stacje robocze i we wszystkie stacje robocze serwerów podrzędnych (struktura drzewiasta).
	26. Serwer centralnej administracji ma oferować funkcjonalność synchronizacji grup komputerów z drzewem Active Directory. Po synchronizacji automatycznie są umieszczane komputery należące do zadanych grup w AD do odpowiadających im grup w programie. Funkcjonalność ta nie może wymagać instalacji serwera centralnej administracji na komputerze pełniącym funkcję kontrolera domeny.
	27. Serwer centralnej administracji ma umożliwiać definiowanie różnych kryteriów wobec podłączonych do niego klientów (w tym minimum przynależność do grupy roboczej, przynależność do domeny, adres IP, adres sieci/podsieci, zakres adresów IP, nazwa hosta, przynależność do grupy, brak przynależności do grupy). Po spełnieniu zadanego kryterium lub kilku z nich stacja ma otrzymać odpowiednią konfigurację.
	28. Serwer centralnej administracji ma być wyposażony w mechanizm informowania administratora o wykryciu nieprawidłowości w funkcjonowaniu oprogramowania zainstalowanego na klientach, w tym przynajmniej informowaniu o wygaśnięciu licencji na oprogramowanie, informowaniu o tym, że zdefiniowany procent spośród wszystkich stacji podłączonych do serwera ma nieaktywną ochronę oraz że niektórzy z klientów podłączonych do serwera oczekują na ponowne uruchomienie po aktualizacji do nowej wersji oprogramowania.
	29. Serwer centralnej administracji ma być wyposażony w wygodny mechanizm zarządzania licencjami, który umożliwi sumowanie liczby licencji nabytych przez użytkownika. Dodatkowo serwer ma informować o tym ilu stanowiskową licencję posiada użytkownik i stale nadzorować ile licencji spośród puli nie zostało jeszcze wykorzystanych.
	30. W sytuacji, gdy użytkownik wykorzysta wszystkie posiadane licencje po zakupie oprogramowania, administrator po zalogowaniu się do serwera poprzez konsolę administracyjną musi zostać poinformowany o tym fakcie za pomocą okna informacyjnego.
	31. Możliwość tworzenia repozytorium aktualizacji na serwerze centralnego zarządzania i udostępniania go przez wbudowany serwer http.
	32. Aplikacja musi posiadać funkcjonalność, która umożliwi dystrybucję aktualizacji za pośrednictwem szyfrowanej komunikacji (za pomocą protokołu https).
	33. Do aktualizacji za pośrednictwem protokołu https nie może być wymagane instalowanie dodatkowych zewnętrznych usług jak IIS lub Apache zarówno od strony serwera aktualizacji jak i klienta.
	34. Dostęp do kwarantanny klienta musi być z poziomu systemu centralnego zarządzania.
	35. Możliwość przywrócenia lub pobrania zainfekowanego pliku ze stacji klienckiej przy wykorzystaniu centralnej administracji.
	36. Administrator musi mieć możliwość przywrócenia i wyłączenia ze skanowania pliku pobranego z kwarantanny stacji klienckiej.
	37. Podczas przywracania pliku, administrator musi mieć możliwość zdefiniowania kryteriów dla plików, które zostaną przywrócone, w tym minimum: zakresu czasu z dokładnością co do minuty kiedy wykryto daną infekcję, nazwy danego zagrożenia, dokładnej nazwy wykrytego obiektu oraz zakresu minimalnej i maksymalnej wielkości pliku z dokładnością do jednego bajta.
	38. Możliwość utworzenia grup, do których przynależność jest aplikowana dynamicznie na podstawie zmieniających się parametrów klientów, w tym minimum w oparciu o: wersję bazy sygnatur wirusów, maskę wersji bazy sygnatur wirusów, nazwę zainstalowanej aplikacji, dokładną wersję zainstalowanej aplikacji, przynależność do domeny lub grupy roboczej, przynależność do serwera centralnego zarządzania, przynależność lub jej brak do grup statycznych, nazwę komputera lub jej maskę, adres IP, zakres adresów IP, przypisaną politykę, czas ostatniego połączenia z systemem centralnej administracji, oczekiwanie na restart, ostatnie zdarzenie związane z wirusem, ostatnie zdarzenie związane z usługą programu lub jego procesem, ostatnie zdarzenie związane ze skanowaniem na żądanie oraz z nieudanym leczeniem podczas takiego skanowania, maską wersji systemu operacyjnego oraz flagą klienta mobilnego.
	39. Podczas tworzenia grup dynamicznych, parametry dla klientów można dowolnie łączyć oraz dokonywać wykluczenia pomiędzy nimi.
	40. Utworzone grupy dynamiczne mogą współpracować z grupami statycznymi.
	41. Możliwość definiowania administratorów o określonych prawach do zarządzania serwerem administracji centralnej (w tym możliwość utworzenia administratora z pełnymi uprawnieniami lub uprawnienia tylko do odczytu).
	42. W przypadku tworzenia administratora z niestandardowymi uprawnieniami, możliwość wyboru modułów, do których będzie posiadał uprawnienia, tj.: zarządzanie grupami, powiadomieniami, politykami, licencjami, usuwanie i modyfikacja klientów, zdalna instalacja, generowanie raportów, usuwanie logów, zmiana konfiguracji klientów, aktualizacja zdalna, zdalne skanowanie klientów, zarządzanie kwarantanną na klientach.
	43. Możliwość synchronizowania użytkowników z Active Directory w celu nadania uprawnień administracyjnych do serwera centralnego zarządzania.
	44. Wszystkie działania administratorów zalogowanych do serwera administracji centralnej mają być logowane.
	45. Możliwość uruchomienia panelu kontrolnego dostępnego za pomocą przeglądarki internetowej.
	46. Panel kontrolny musi umożliwiać administratorowi wybór elementów monitorujących, które mają być widoczne.
	47. Administrator musi posiadać możliwość tworzenia wielu zakładek, w których będą widoczne wybrane przez administratora elementy monitorujące.
	48. Elementy monitorujące muszą umożliwiać podgląd w postaci graficznej co najmniej: bieżącego obciążenia serwera zarządzającego, statusu serwera zarządzającego, obciążenia bazy danych, z której korzysta serwer zarządzający, obciążenia komputera, na którym zainstalowana jest usługa serwera zarządzającego, informacji odnośnie komputerów z zainstalowaną aplikacją antywirusową, a które nie są centralnie zarządzane, podsumowania modułu antyspamowego, informacji o klientach znajdujących się w poszczególnych grupach, informacji o klientach z największą ilością zablokowanych stron internetowych, klientach, na których zostały zablokowane urządzenia zewnętrzne, informacji na temat greylistingu, podsumowania wykorzystywanych systemów operacyjnych, informacji odnośnie spamu sms, zagrożeń oraz ataków sieciowych.
	49. Administrator musi posiadać możliwość maksymalizacji wybranego elementu monitorującego.
	50. Możliwość włączenia opcji pobierania aktualizacji z serwerów producenta z opóźnieniem.
	51. Możliwość przywrócenia baz sygnatur wirusów wstecz (tzw. Rollback).
	52. Aplikacja musi mieć możliwość przygotowania paczki instalacyjnej dla stacji klienckiej, która będzie pozbawiona wybranej funkcjonalności.
	53. Wsparcie dla protokołu IPv6.
	54. Administrator musi posiadać możliwość centralnego, tymczasowego wyłączenia wybranego modułu ochrony na stacji roboczej.
	55. Centralne tymczasowe wyłączenie danego modułu nie może skutkować koniecznością restartu stacji roboczej.
	56. Aplikacja musi posiadać możliwość natychmiastowego uruchomienia zadania znajdującego się w harmonogramie bez konieczności oczekiwania do jego zaplanowanego czasu.
	57. Aplikacja do administracji centralnej musi umożliwiać utworzenie nośnika, za pomocą którego będzie istniała możliwość przeskanowania dowolnego komputera objętego licencją przed startem systemu.
	58. Administrator musi posiadać możliwość określenia ilości jednoczesnych wątków instalacji centralnej oprogramowania klienckiego.

W przypadku zaoferowania oprogramowania równoważnego do posiadanego przez zamawiającego, celem potwierdzenia spełniania przez oferowane oprogramowanie wymagań określonych przez zamawiającego, wykonawca dołączy do oferty specyfikacje techniczne oferowanego oprogramowania.Specyfikacje techniczne muszą być sporządzone w języku polskim. W przypadku dokumentów sporządzonych w języku obcym, wykonawca składa je wraz z tłumaczeniem na język polski, poświadczonym przez wykonawcę. |

**Program do zdalnej kontroli i zdalnego współdzielenia pulpitu przez internet**

|  |
| --- |
| Licencja na 1 rok (od 22 listopada 2015 r.) |
| Liczba stanowisk roboczych umożliwiających uruchomienie sesji zdalnego sterowania lub udział w meetingu | nieograniczona |
| Liczba jednoczesnych sesji zdalnego sterowania lub meetingów | 1 |
| Rozwiązanie do wielu zastosowań: zdalnego dostępu, meetingów, prezentacji, zdalnego zarządzania komputerami lub serwerami. |
| Pracuje w systemach Windows, iPhone/iPad i Android, umożliwia połączenia między platformami. |
| Nie wymaga konfiguracji, działa poprzez zapory ogniowe i serwery proxy. |
| Dźwięk i obraz z komputera zdalnego. |
| Rejestrowanie sesji zdalnego sterowania lub meetingów z dźwiękiem i połączeniami VoIP oraz konwerter obrazu do formatu AVI. |
| Proste zarządzanie partnerami za pomocą listy Komputerów i kontaktów, łączenie jednym kliknięciem. |
| Możliwość sprawdzenia na liście Komputerów i kontaktów, które komputery i kontakty są aktualnie podłączone i dostępne. |
| Komunikator wbudowany w listę Komputerów i kontaktów – czat z kilkoma osobami równocześnie, wysyłanie wiadomości w trybie offline. |
| Obsługa środowiska Terminal Server: możliwość przypisania niezależnego identyfikatora każdemu użytkownikowi. W ten sposób, użytkownicy mogą korzystać z programu równocześnie i niezależnie od siebie. |
| Bezpośrednie połączenia lokalne z użyciem protokołu TCP/IP, nawet bez dostępu do internetu. |
| Możliwość zdalnego korzystania z przycisków specjalnych (np. Ctrl+Alt+Del). |
| Instalacja w postaci usługi systemowej. |
| Zmiana kierunku połączenia: odwracanie kierunku przeglądania w czasie trwania połączenia. |
| Funkcja Przeciągnij i upuść do przesyłania plików w dwóch kierunkach, do wybranej lokalizacji. |
| Aplikacje dla systemów iOS i Android umożliwiają sterowanie zdalnym komputerem i przesyłanie plików w obie strony przy pomocy urządzeń mobilnych. |
| Obsługa kilku monitorów - wygodne przechodzenie między monitorami. Możliwość równoczesnego wyświetlania zdalnych ekranów na ekranie komputera lokalnego (np. 2 okien na 2 monitorach).  |
| Swobodne skalowanie okna zdalnego sterowania. |
| Zapisywanie ustawień połączeń dla łatwiejszego łączenia się z tymi samymi grupami, kontaktami lub komputerami. |
| Funkcja wykonywania zrzutów ekranu podczas sesji zdalnego sterowania. |
| Wyświetlanie informacji o systemie zainstalowanym na zdalnym komputerze. |
| Sterowanie zdalnymi komputerami za pośrednictwem przeglądarki, bez potrzeby instalacji specjalnego oprogramowania (odczyt plików HTML i Flash). |
| Szerokie możliwości zarządzania użytkownikami: tworzenie, edycja, blokowanie i zarządzanie hasłami każdego użytkownika. |
| Rozbudowane możliwości tworzenia raportów z połączeń. |
| Obsługa klawiatury międzynarodowej. |
| Automatyczna instalacja aktualizacji. |
| Zabezpieczenia (SSL): wymiana kluczy publicznych i prywatnych RSA oraz szyfrowanie sesji 256-bitowym kodem AES. |

**CZĘŚĆ 2.**

**Zakup i wdrożenie Forti Analyzer 200D**

|  |
| --- |
| Oferowany produkty musi spełniać wszystkie parametry określone w niniejszym załączniku oraz być fabrycznie nowy, oznakowany symbolem CE, pochodzić z legalnego źródła, musi być dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju i objęty standardowym pakietem usług gwarancyjnych zawartym w cenie urządzenia i oprogramowania świadczonym przez sieć serwisową producenta na terenie Polski.  |

|  |
| --- |
| **Centralne logowanie i korelacja**1. System centralnego logowania musi współpracować z posiadanym systemem bezpieczeństwa opartego o platformę FortiGate 200B.
2. Elementy systemu bezpieczeństwa odpowiedzialne za zarządzanie i monitoring mają umożliwiać centralizację procesów zarządzania wszystkimi funkcjonalnościami elementów realizujących funkcje bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.
3. W ramach systemu logowania i raportowania dostawca powinien dostarczyć spójny system monitorujący, gromadzący logi, korelujący zdarzenia i generujący raporty na podstawie danych ze wszystkich elementów systemu bezpieczeństwa.
4. Platforma powinna dysponować predefiniowanym zestawem przykładów raportów, dla których administrator systemu będzie mógł modyfikować parametry prezentowania wyników.
5. System centralnego logowania i raportowania powinien być dostarczony w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
6. W ramach centralnego systemu logowania, raportowania i korelacji powinny być realizowane poniższe funkcjonalności:
7. Konfigurowalne opcje powiadamiania o zdarzeniach jak. email, SNMP
8. Podgląd logowanych zdarzeń w czasie rzeczywistym.
9. Generowanie raportów w zakresie wszystkich funkcjonalności bezpieczeństwa realizowanych przez system - na żądanie oraz w trybie cyklicznym, w postaci popularnych formatów min: PDF. Raporty powinny obejmować zagadnienie dotyczące całej sfery bezpieczeństwa.
10. Zastosowane systemy logowania powinny umożliwiać cykliczny eksport zgromadzonych logów do zewnętrznych systemów przechowywania danych w celu ich długo czasowego składowania.
11. Na podstawie analizy przeprowadzonych testów w zakresie ilości logów w ciągu sekundy, zastosowany system centralnego logowania powinien umożliwiać zapis oraz analizę co najmniej 200 nowych logów/sekundę.
12. System powinien dysponować co najmniej 4 interfejsami Ethernet 10/100/1000 oraz powierzchnią dyskową min. 1 TB.
 |
| **Usługa wdrożenia** W zakres zamówienia wchodzi oprócz dostawy wyspecyfikowanych urządzeń, także ich wdrożenie na miejscu u zamawiającego przez producenta lub certyfikowanego do tego przez producenta partnera**Konfiguracja**:1. Konfiguracja UTM
2. Instalacja oraz konfiguracja centralnego systemu logowania i raportowania
3. Konfiguracja raportów
4. Testy
5. Włączenie systemu do raportowania do środowiska produkcyjnego
6. Monitoring
7. Szkolenie administratorów
 |

**Odnowienie licencji i przedłużenie usług wsparcia VMware**

|  |
| --- |
| Przedmiotem zamówienia jest odnowienie licencji i przedłużenie usług wsparcia technicznego dla posiadanego przez WUP Poznań oprogramowania VMware, do dnia 13 października 2018 r. Kalkulację cenową należy przedstawić według poniższej specyfikacji:1. 1 komplet licencji dla 3 serwerów 2 procesorowych;
2. VMware vSphere 5 Essentials Plus w opcji Basic Support and Subscription;
3. Contract #45437698
 |

**Załącznik nr 2 do SIWZ**

**FORMULARZ OFERTY**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*ZAMAWIAJĄCY –* **Wojewódzki Urząd Pracy w Poznaniu**

**ul. Kościelna 37, 60-537 Poznań;**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Nazwa (Firma) Wykonawcy –

……………………………………………………………………………………………………...,

Adres siedziby –

……………………………………………………………………………………………………...,

Adres do korespondencji –

……………………………………………………………………………………........................,

Tel. - ......................................................; fax - ......................................................;

E-mail: ..............................................................;

NIP - .................................................; REGON - .................................................;

 W odpowiedzi na ogłoszenie o postępowaniu o udzielenie zamówienia w trybie przetargu nieograniczonego na dostawę sprzętu komputerowego i oprogramowania
dla Wojewódzkiego Urzędu Pracy w Poznaniu, oświadczamy że:

* + - 1. Składamy ofertę na wykonanie przedmiotu zamówienia w zakresie określonym w SIWZ
			i oświadczamy, że złożona przez nas oferta spełnia wszystkie wymogi w niej zawarte,
			za cenę całkowitą:

**Część 1**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa** | **Ilość** | **Cena jedn. netto w zł.** | **Wartość netto w zł** | **Wartość brutto w zł** |
| 1. | Zestaw komputerowy wraz z oprogramowaniem | 16 |  |  |  |
| Producent ………………………………………………………………………………………………..Model/typ ……………………………………………………………………………………………….. |
| 2. | Aktualizacja i rozszerzenie oprogramowania antywirusowego na stacje robocze i serwery wraz z konsolą do centralnej administracji  | aktualizacje | 310 |  |  |  |
| nowe licencje | 7 |  |  |  |
| Nazwa oprogramowania ……………………………………………………………………………….. |
| 3. | Program do zdalnej kontroli i zdalnego współdzielenia pulpitu przez internet | 1 |  |  |  |
| Nazwa oprogramowania ……………………………………………………………………………….. |
| **Razem** |  |  |

**Udzielamy …….. miesięcznego okresu gwarancji na zestawy komputerowe – poz. 1.**

**Razem oferowana wartość brutto** ……………………. zł

(słownie: …………………………………………………….…………………….złotych):

**Część 2**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa** | **Ilość** | **Wartość netto** **w zł** | **Wartość brutto** **w zł** |
| 1. | Zakup i wdrożenie Forti Analyzer 200D | 1 |  |  |
| 2. | Odnowienie licencji i przedłużenie usług VMware | 1 |  |  |
| **Razem** |  |  |

**Oferujemy dostawę urządzenia z poz. 1 w terminie ………dni kalendarzowych
od daty zawarcia umowy.**

**Razem oferowana wartość brutto** ……………………. zł

(słownie: …………………………………………………….…………………….złotych):

1. W przypadku udzielenia zamówienia, zobowiązujemy się do zawarcia umowy w miejscu
i terminie wskazanym przez Zamawiającego oraz na warunkach określonych w istotnych postanowieniach umowy stanowiących integralną część SIWZ.
2. Oświadczamy, że jeżeli w okresie związania ofertą nastąpią jakiekolwiek znaczące zmiany sytuacji przedstawionej w naszych dokumentach załączonych do oferty, natychmiast poinformujemy o nich Zamawiającego.
3. Oświadczamy, że jesteśmy związani niniejszą ofertą przez okres 30 dni, który rozpoczyna się wraz z upływem terminu składania ofert.
4. Oferta wraz z załącznikami została złożona na ….. stronach.
5. Niniejszym informujemy, że informacje składające się na ofertę, zawarte na stronach …..... stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy
o zwalczaniu nieuczciwej konkurencji ze względu na następujące okoliczności\*:……………………………………………………………………………………………………………………………………………………………………………………………….

⃰ Wykonawca winien wykazać zastrzeżenie powyższych informacji

1. Do oferty załączamy następujące dokumenty:

1) ……………………………………………...........................................................................

2) ……………………………………………...........................................................................

3) ……………………………………………...........................................................................

 …………………………………………

 (pieczęć i podpis osoby uprawnionej do składania oświadczeń woli
 w imieniu wykonawcy)

Miejscowość …......................................... dnia …........................................ roku.

**Załącznik nr 3 do SIWZ**

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

 (pieczęć firmowa Wykonawcy)

OŚWIADCZENIE O SPEŁNIANIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU
OKREŚLONYCH W ART. 22 UST. 1 USTAWY PRAWO ZAMÓWIEŃ PUBLICZNYCH

Przystępując do postępowania o udzielenie zamówienia publicznego prowadzonego
w trybie przetargu nieograniczonego na dostawę sprzętu komputerowego i oprogramowania
dla Wojewódzkiego Urzędu Pracy w Poznaniu, w imieniu Wykonawcy wskazanego powyżej oświadczam/y, że spełniam/y warunki dotyczące:

* 1. posiadania uprawnień do wykonania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania,
	2. posiadania wiedzy i doświadczenia,
	3. dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi
	do wykonania zamówienia,
	4. sytuacji ekonomicznej i finansowej.

 …………………………………………

 (pieczęć i podpis osoby uprawnionej do składania oświadczeń woli
 w imieniu wykonawcy)

Miejscowość …......................................... dnia …........................................ roku.

**Załącznik nr 4 do SIWZ**

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

 (pieczęć firmowa Wykonawcy)

OŚWIADCZENIE O BRAKU PODSTAW DO WYKLUCZENIA Z POSTĘPOWANIA
O UDZIELENIE ZAMÓWIENIA W OKOLICZNOŚCIACH, O KTÓRYCH MOWA
W ART. 24 UST. 1 USTAWY PRAWO ZAMÓWIEŃ PUBLICZNYCH

Przystępując do postępowania o udzielenie zamówienia publicznego prowadzonego
w trybie przetargu nieograniczonego na dostawę sprzętu komputerowego i oprogramowania
dla Wojewódzkiego Urzędu Pracy w Poznaniu, w imieniu Wykonawcy wskazanego powyżej oświadczam/y, że:

Nie podlegam/y wykluczeniu na podstawie art. 24 ust. 1 ustawy Prawo zamówień publicznych.

 …………………………………………

 (pieczęć i podpis osoby uprawnionej do składania oświadczeń woli
 w imieniu wykonawcy)

Miejscowość …......................................... dnia …........................................ roku.

**Załącznik nr 5 do SIWZ**

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

 (pieczęć firmowa Wykonawcy)

INFORMACJA WYKONAWCY DOTYCZĄCA PRZYNALEŻNOŚCI

DO GRUPY KAPITAŁOWEJ

Przystępując do postępowania o udzielenie zamówienia publicznego prowadzonego
w trybie przetargu nieograniczonego na dostawę sprzętu komputerowego i oprogramowania
dla Wojewódzkiego Urzędu Pracy w Poznaniu, oświadczam/y, że Wykonawca:

* nie należy do grupy kapitałowej\*
* należy do grupy kapitałowej i w załączeniu składa listę podmiotów należących do tej samej grupy kapitałowej\*

**\* właściwe zakreślić**

 …………………………………………

 (pieczęć i podpis osoby uprawnionej do składania oświadczeń woli
 w imieniu wykonawcy)

Miejscowość …......................................... dnia …........................................ roku.

**Załącznik nr 6 do SIWZ**

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

 (pieczęć firmowa Wykonawcy)

**WYKAZ GŁÓWNYCH DOSTAW**

Przystępując do postępowania o udzielenie zamówienia publicznego prowadzonego
w trybie przetargu nieograniczonego na dostawę sprzętu komputerowego i oprogramowania
dla Wojewódzkiego Urzędu Pracy w Poznaniu, w imieniu Wykonawcy wskazanego powyżej przedstawiam/y, wykaz wykonanych lub wykonywanych głównych usług:

**Część 1**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Podmiot na rzecz którego wykonano dostawę** | **Przedmiot zamówienia** | **Termin wykonania/ wykonywania zamówienia**.…/…./….(dzień/miesiąc/rok) | **Wartość (w zł brutto)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Załączniki:

dowody, że ww. dostawy zostały wykonane lub są wykonywane należycie

**Część 2**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Podmiot na rzecz którego wykonano dostawę** | **Przedmiot zamówienia** | **Termin wykonania/ wykonywania zamówienia**.…/…./….(dzień/miesiąc/rok) | **Wartość (w zł brutto)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Załączniki:

dowody, że ww. dostawy zostały wykonane lub są wykonywane należycie

 …………………………………………

 (pieczęć i podpis osoby uprawnionej do składania oświadczeń woli
 w imieniu wykonawcy)

Miejscowość ............................................ dnia ........................................... roku.

**Załącznik nr 7 do SIWZ**

**Dot. Części 2**

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

*(Pieczęć firmowa Wykonawcy)*

**WYKAZ OSÓB PRZEWIDZIANYCH DO REALIZACJI PRZEDMIOTU ZAMÓWIENIA**

Przystępując do postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na dostawę sprzętu komputerowego i oprogramowania
dla Wojewódzkiego Urzędu Pracy w Poznaniu, w imieniu Wykonawcy wskazanego powyżej, przedstawiam/y wykaz osób, które będą uczestniczyć w wykonywaniu zamówienia:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Imię i nazwisko** | **Wykształcenie** | **Kwalifikacje** | **Certyfikaty producenta systemów raportowania i logowania** | **Zakres****powierzonych****do wykonania****czynności** | **Informacja****o podstawie****do dysponowania****osobą przez****Wykonawcę** |
| 1. |  |  |  |  |  |  |
| 2. |  |  |  |  |  |  |
| … |  |  |  |  |  |  |

Oświadczam, że wskazane wyżej osoby:

* + - 1. spełniają wymagania, o których mowa w SIWZ,
			2. posiadają praktyczne doświadczenie z zakresu odpowiadającego zakresowi przedmiotowemu zamówienia,

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

 (pieczęć i podpis osoby uprawnionej do składania oświadczeń woli
 w imieniu Wykonawcy)

Miejscowość ............................................. dnia ...............................................roku.

1. umieszczenie treści uzależnione od oświadczenia Wykonawcy [↑](#footnote-ref-1)
2. umieszczenie treści uzależnione od oświadczenia Wykonawcy [↑](#footnote-ref-2)
3. Długość gwarancji uzależniona od oświadczenia Wykonawcy wskazanego w ofercie. [↑](#footnote-ref-3)
4. Termin wykonania przedmiotu umowy uzależniony od oświadczenia Wykonawcy wskazanego w ofercie. [↑](#footnote-ref-4)
5. umieszczenie treści uzależnione od oświadczenia Wykonawcy [↑](#footnote-ref-5)
6. umieszczenie treści uzależnione od oświadczenia Wykonawcy [↑](#footnote-ref-6)
7. - rozwiązanie równoważne zgodne z systemem Windows 7 Professional, zapewniające kompatybilność (bezpieczeństwo, stabilność i wydajność) nowych komputerów z wykorzystywanymi przez Zamawiającego rozwiązaniami stworzonymi pod system Windows Ww. oprogramowanie systemowe (rozwiązanie równoważne) powinno zapewnić poprawną obsługę wszystkich powszechnie używanych urządzeń peryferyjnych (drukarek, skanerów, kserokopiarek). Jeżeli ze względu na zaoferowane oprogramowanie zaistnieje konieczność poniesienia przez Zamawiającego dodatkowych nakładów (szkolenie pracowników, zwiększenie dotychczasowej czasochłonności przygotowania stanowisk komputerowych, zmian konfiguracji usług sieciowych) niezbędnych do sprawnego funkcjonowania stacji roboczych w infrastrukturze teleinformatycznej Zamawiającego, wszelkie koszty z tym związane poniesie Wykonawca. [↑](#footnote-ref-7)
8. - równoważny tj. zapewniający pełną funkcjonalność oraz wygląd dokumentów stworzonych przez Microsoft Office 2013, 2010, 2007, 2003 (np. poprawne działanie makr z aplikacji Excel, obsługa skryptów VB) identycznie jak w Microsoft Office 2013. Zapewniający poprawną obsługę nakładek systemowych w ramach aplikacji PEFS. Dokument stworzony w równoważnym pakiecie biurowym powinien posiadać wygląd oraz funkcjonalność jak w pakietach biurowych Microsoft Office. [↑](#footnote-ref-8)